International Journal of Engineering & Technology, 7 (2) (2018) 768-771

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET
doi: 10.14419/ijet.v7i2.10106
Research paper

A secure dynamic adaptive routing technique using game theory in wireless sensor network

Muruganandam. A [1] *, Dr. Anitha. R [2]

[1] Research Scholar, Department of Computer Science, Bharathiar University, Coimbatore, TamilNadu, India
[2] Research Supervisor, Department of MCA, Muthayammal Engineering College, Rasipuram, Nammakkal, TamilNadu, India
**Corresponding author E-mail: murugandbc1976@gmail.com*

Abstract

A Wireless Sensor Network (WSNs) is popular developing the field in industrial and other major markets. Wireless data security is the central theme in the WSNs application where security of transmitted data is more concerned. Due to the significant concentration of energy efficiency and performance analysis in WSN, providing secured communication is a challenging issue. To overcome this interdependent problem Game theory can be used. Game theory is applied here to select different routes to transfer the data from source to destination. The performance of the WSNs can be increased by providing security for transmitted data. The graph for throughput, end to end delay, delivery, and packet loss ratio are generated using NS2 simulation tool.

Keywords: *DSR; Energy Efficient; Game theory; NS2; Wireless Sensor Networks.*

1. Introduction

A Wireless Sensor Networks (WSNs) is the combination of sensor nodes networked together to collect and process the sensed values and transmit the collected results to the base station through wireless transmitters. Each sensor nodes consists of four important segments. They are the sensor unit, the power supply unit, the processing unit and the transceiver unit. These sensor nodes broadcast the sensed values to other nodes to route the information to the base station or else for their analysis. Wireless Sensor Networks (WSNs) nodes mostly comprise primary sensors that measure light, pressure, sound and other parameters of placed environment. The nodes are powered with small batteries. Since Wireless Sensor Networks (WSNs) are placed in sensing field, replacing of power source manually is difficult and expensive. Due to this limited power source, energy efficiency plays a significant role in Wireless Sensor Networks (WSNs).

In Wireless Sensor Networks (WSNs), many security protocols have been proposed to overcome the security threats, but there are still limitations to overcome the security related problems. Traditional cryptographic methods hold a bigger encryption technique that affects the memory conception, battery conception and inhibit the performance of network

Communication Wireless sensor networks have limited network lifetime and hence network protocols used in it must focus on improving the performance of the system.

Every node present in a network plays a dual role. The first consists of sensing the environment and transfer of the sensed value to the base station or the sink node. The second is to continue its life to the extent possible. This naturally creates a robust environment enabling maintenance of energy efficiency and secured communication in major criteria. So designing the network protocol is very important. Here we introduce the Game theory for overcoming security threats and energy maintenance in wireless sensor networks.

2. Related work

Wireless Sensor Networks (WSNs) are used in many important areas like military surveillance and forest fire control. They use multi-hop routing to transfer the data efficiently to the sink node or base station. Identity theft is avoided by implementing multi-hop information in routing data and provide maximum protection against identity deception. Authentication of trusty nodes is highly important in major applications like military surveillance and industrial Wireless Sensor Networks (WSNs). Provision of secured communication is the central theme of research in Wireless Sensor Networks (WSNs). Trust-aware routing protocols available currently are not more efficient to obviate theft of transmitted data. The cryptography techniques used in this affects the performance of networks, energy efficiency or any relevant factors. Fuzzy logic is implemented for overcoming this problem and to perform trusting operation in Wireless Sensor Networks routing. This is along with Bio inspired Energy Efficiency cluster protocol for determination of the threshold values meant for locating the trust worthiness of a node. A table has been generated, and the trust values of each node are compared with the threshold value. If the value is high, the node is saved as a trusted node and added to the table or else, the node is considered as an untrusted node and not placed in the routing table. This helps us to avoid black hole and flooding attacks. [1].

Most of the Wireless Sensor Networks (WSNs) applications are battery powered. Energy management has a vital role to play in view of the low volume of the available power. Many types of research are proposed monitoring and control of the energy management for Wireless Sensor Networks (WSNs). The energy aware framework designed now a day is not efficient as they are designed on the basis of the software environment. The requirements and challenges provided by software environment are not complicated when compared to real-time issues. So most of the

energy monitoring frameworks produce small results when implemented in real time environment. Here we introduce the multi-channel Energy Measurement device, Energy Data Management software and testing nodes. These together generate, the energy management issues in test bed node in real time environment and produce results. These measurements help researchers to get a clear of the required efficient protocol using the results of our test bed. [2].

A combined network with Wireless Sensor Networks and cloud computing has been produced for overcoming the issues relating to storage, real time processing and challenges in battery or node size and characteristics or Wireless Sensor Networks nodes. This combination solves the problems mentioned above but still generates an issue in the security of data in cloud storage. To overcome this problem pub/sub framework is implemented. This structure provides the maximum level of safety for the data stored in the cloud storage. By sharing the process between the cloud and Wireless Sensor Networks (WSNs), it increases the performance and speed of the network. [3]

Wireless Sensor Networks (WSNs) constitute a fast growing technology. Many research studies are now a foot one the subjects of getting elongated network life time and bringing down energy consumption. Energy efficient protocols play a significant role in increasing network lifetime. Here we introduce Linear Cluster Handling Technique (LCH) for maintaining the energy efficiency in multi-static sink nodes in Wireless Sensor Networks (WSNs). The system is divided into four regions, placing four static sink nodes at all corners for efficient collection of data from the network nodes. Distributed Energy Efficient Clustering with Linear Cluster Handling (DEEC-LCH) is used to maintain energy efficient routing protocol in the network. The energy efficiency of this technique is monitored in the software environment. Another method named Threshold Sensitive Energy Efficient with Linear Cluster Handling (TEEN-LCH) is also implemented in three static sink nodes scenario. The combined performance of these two techniques is analyzed for network lifetime, throughput and net energy consumption. [4]

Homogeneous Wireless Sensor Networks (HWSNs) is one of the major fields in WSNs. It deals with the hardware configuration that possess limited resource and processing capacity. The hardware environment possesses unique characteristics for focus on higher security in applications. Additional light weight security models have been proposed for overcoming security threats. These are based on a specific hardware attack. Here we introduce a clustering based key management scheme. Our security system develops a higher efficient security method compared to disjointed clusters. These clusters are made to combine by the randomly selected nodes. This provides analysis for both nodes connectivity and the safety from capture attack. [5]

Wireless Sensor Networks (WSNs) find many applications, in military, natural, and well-being related zones. These applications regularly incorporate the checking of accurate data, for example, for development in the war zone or the area of staff in a building. Security is essential in Wireless Sensor Networks (WSNs). Then again, Wireless Sensor Networks (WSNs) experience the ill effects of numerous imperatives, including low calculation ability, little memory, restricted vitality assets, powerlessness to real catch, and the utilization of shaky remote correspondence channels. These limitations fuse a challenge to security in Wireless Sensor Networks (WSNs). The authors have, in this paper, made an attempt to investigate safety issues in Wireless Sensor Network. Initially, the imperatives, security prerequisites and attacks with their comparing countermeasures in Wireless Sensor Networks (WSNs) are clarified. Singular sensor hubs are liable to trade off security. An attacker can infuse false reports into the systems using traded off hubs. Besides, a foe can make a Gray gap by traded off hubs. If these two sorts of attacks happen simultaneously in a system, a percentage of the current strategies neglect to safeguard against those attacks. The Ad-hoc On Demand Distance (AODV) Vector plan for recognizing Gray-Hole assault and Statistical En-Route Filtering is utilized for locating false report. Elliptic curve cryptography is employed for improvement of the security level. [6]

Energy efficiency and fault tolerance play a vital role in WSNs. When the nodes communicate with the node far away, it spends considerable energy to transfer the data to the receiver node. Communication distance requires to be minimized for overcoming this problem as also that of loss of energy for the routing data. Node failure is inevitable despite the monitoring of energy consumption. A node in Wireless Sensor Networks (WSNs) can malfunction or get hacked by an attacker. So the transmitting node can tend to transmit data to longer distance. This leads to loss of network lifetime. Energy hole aware efficient communication is introduced for overcoming this problem. This methods solves the energy hole problem and increases energy efficiency. [7]

SAERP: An Energy Efficiency Real-time Routing Protocol in Wireless Sensor Networks (WSNs) is widely used for sensor communication. In this paper the dynamic network sustenance for critical issues such as bandwidth operation, a control system is discussed. A Simultaneous Attentive Energy Routing Protocol (SAERP) is used for improvement of the dynamic network sustenance [8].

Wireless Sensor Networks (WSNs) is widely used for monitoring environmental conditions. Since Wireless Sensor Networks (WSNs) operate in an open environment, they are prone to security threats. The cryptographic method does not suffer from any limitation due to the nature of Wireless Sensor Networks. A novel algorithm has been used in this paper for prevention of node compromise, and internal attack from the compromised node, using the multi-hop and single sinker. The algorithm is based on the proposed algorithm was implemented on an actual test bed to support the claim [9].

Improved Energy Efficiency Semi-Static Routing (EESSR) algorithm using sink mobility for Wireless Sensor Networks (WSNs) ubiquitous wireless sensor network devices are battery powered, and so network lifetime and energy management is an important issue. One way to improve the network lifetime is the use of Energy Efficiency Semi-Static Clustering (EESSC) protocol is used to form node clusters. In this paper developed Energy Efficiency Semi-Static Routing is proposed which is simulated, and the results are compared with EESSC and LEACH based on individual network constraints such as network lifetime and middle node death. Experimental results show that the proposed method is better than EESSC and LEACH [10].

3. Problem of the statement

Energy efficiency and performance analysis in wireless sensor network is a challenging issue for providing secured communication in sensor network. To overcome this problem the researchers used the Game theory approach.

4. Motivation

Game theory is a new concept suggested for wireless sensor networks can be improved by providing data security for transmitted data and ensuring energy efficiency. This theory is applied for the partitioning of data and then selecting the different routes to transfer data from source to destination. It is also possible for uniform utilisation of energy resource in the sensor node.

5. Methodology

Electronics and wireless technologies are fast growing techs of Wireless Sensor Networks (WSNs). The proposed work stimulates the concept of data security and energy efficiency in Wireless Sensor Networks (WSNs) applications. A new concept named the game theory in Wireless Sensor Networks for providing data security and ensuring energy efficiency. In addition to Game Theory, Dynamic Source Routing (DSR) protocol is implementing to

transmit the data from sender to destination nodes. Dynamic Source Routing is used for establishment of the route between the sender node and receiver node and producing a table of paths through which the data can be successfully transmitted to the sink node. The Game theory can change the paths alternatively to the sink node. The path is not constant and so no one can predict the actual path of the data is transmitted in the network. Along with the different path selection, we also split the packets into multiple pieces and transmit each portion in one direction. So the load for transmission is reduced the data will get fused and split several times while passing through the network. At the destination node, the split data are collected and combined to generate a complete data. This method has the capably of providing maximum security for the transmitted data. An attacker can never collect all the pieces of encoded data to get complete information about the transmitted data. DSR protocol ensures an effective communication link and mitigating packet loss. When the network is big, the process will be more complicated and so the security for the data increases. Reduction in transmission energy is possible as a result of lower packet size network lifetime can also increase.

5.1. Algorithm

Step1: Create source and destination nodes.
Step2: Route between the source and destination nodes are tabled using DSR protocol.
Step3: Count number of possible routes in every hop in the network.
Step4: The data packets are split into some available routes.
Step5: The data was transmitted to next layer or hops.
Step6: Check for destination in the next hop if destination present sends packets to the destination node else split the collected data packets to make ready for next hop.
Step7: Collect and merge the data packets obtained from past hops and split the received data for next hop.
Step8: Continue the steps of splitting and merging of data in several hops until finding the destination node.

5.2. Network simulation tool

Subsequent to the installation of NS2, it is used for evaluate and simulate work apart from other tools used. The Network Simulator is an Object Oriented Simulator, and it can be written in C++ language. The development of NS2 codes are done by using both OTcl (Object oriented extension of Tool Command Language) and C++. Trace Graph is an essential part for displaying a result, so we plot a graph to show a various result comparison with packets, throughput, delivery ratio, network delay and energy efficiency etc. The results are achieved by using Xgraph tool. The proposed and existing methods are compared through the graphs generated.

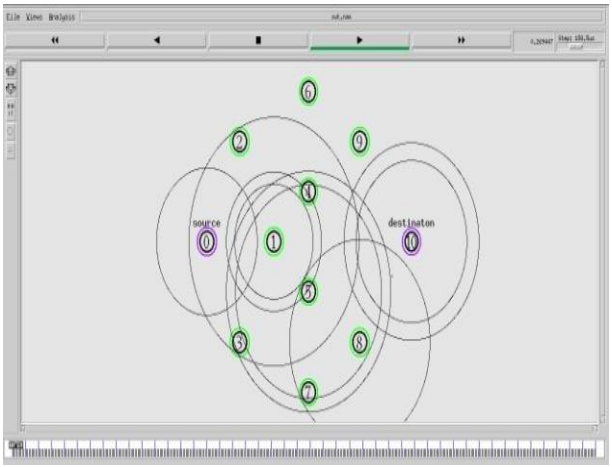

Fig. 1: NS2 Node Arrangement.

The network is designed using a Network Simulator (ns2) and parameters like throughput, packet loss ratio, packet delivery ratio, an end to end delay are calculated. The above Fig. 1 shows the node positions of source, destination and relay nodes of our network.

6. Results and discussion

The method we proposed here was implemented over Network Simulator platform with following parameters. The NS2 parameters are shown below.

Table 1: Simulation Parameter

Parameter	Description
Channel/Wireless Channel	;# channel type
Propagation/2Way Ground	;# radio-propagation model
Phy/Wireless Phy	;# network interface type
Mac/802_11	;# MAC type
Queue/DropTail / PriQueue	;# interface queue type
Queue length	; 500 bits
Number of Nodes	; 16
LL	;# link layer type
Omni Antenna	;# antenna model
50	;# max packet in if q
71	;# number of mobile nodes
DSR	;# routing protocol
100	;# X dimension of topography
100	;# Y dimension of topography
45.0s	;# time of simulation end
100J	; initial energy
100 bits	;packet size

The present study work involves implementing by using DSR routing protocols. The performance of DSR routing protocol is evaluated for observance the network speed and maintaining the routing information is maintain at mobile nodes. There are 71 mobile nodes were used in this simulation work. The other parameters like MAC type, interface queue type, and link layer type are analyzing the data packet and handover to the successor. In sensor networks, the radio propagation model decides whether mobile nodes with given distance and their power of transmission. By default it implements through Omni antenna model to gain all direction. It will be propagated from one place to another place in the simulation model. It predicts the behavior of propagation for all similar links under constraint. So, we can easily achieve the loss of path and effective coverage area of a transmitter by using this model. The initial energy of node is 100j (Joule) with the packet size 100 bits and the queue length is 500 bits. The simulation time ends at 45 seconds and X-Y-dimension of topography are used for creating the graph representation with dimension (100X100). The outcome of the simulation is an output trace file that can be used to do data processing such as throughput, end-to-end delay, etc. It can also visualize the simulation with a program called Network Animator.

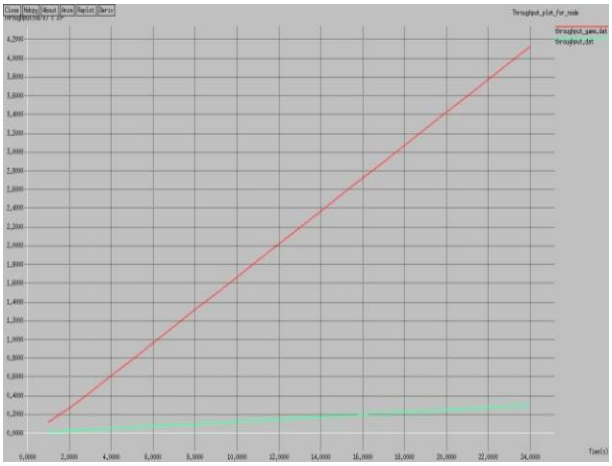

Fig. 2: Throughput.

Fig.2 shows a comparison of throughput for the network created. The red line represents game theory, and the blue line is the existing system without game theory. The data rate is more in proposed method than the existing.

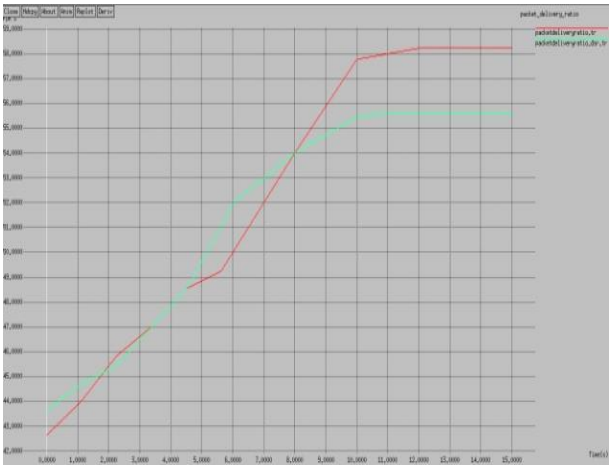

Fig. 3: Packet Delivery Ratios.

Fig.3 shows the Packet delivery ratio that indicates the successful transmission of packets between the sender and the receiver. The ratio of game theory is high when compared to the existing system. Our method attains the maximum delivery ratio in the short time when compared to existing work.

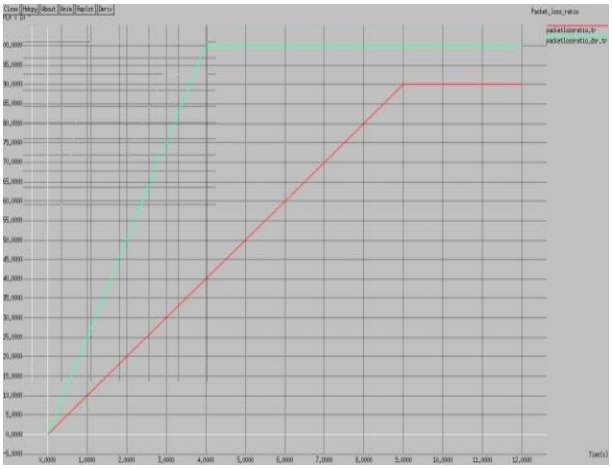

Fig. 4: End to End Delays.

The above Fig. 4 shows the end to end delay in the network. Here the delay in communication between the nodes is reduced when using the game theory. The weightage of data transmission gets reduced consequent on the splitting of data. The reduction is so perpendicular as to ensure reduction in the delay between data transmission through the game theory.

7. Conclusion

This research work provides a detailed view of the Game theory over Wireless Sensor Networks (WSNs) for producing energy efficient and secured protocol. The result generated by our method is compared with the typical Dynamic Source Routing (DSR) network, and it is proved that the Game theory plays the major role in the security of transmitted data's in the network. The combination of Dynamic Source Routing (DSR) and Game theory provides more security than other ethical methods followed in Wireless Sensor Networks (WSNs).

References

[1] S. Renubala, K.S.Dhanalakshmi, "Trust based Secure Routing Protocol using Fuzzy Logic in Wireless Sensor Networks", *Computational Intelligence and Computing Research (ICCIC)*, 2014 IEEE International Conference on 18-20 Dec. 2014. https://doi.org/10.1109/ICCIC.2014.7238435.

[2] N. Zhu, I. O. Connor, U. De Lyon, N. De Lyon, and I. N. L. Umar, "Energy Measurements and Evaluations on High Data Rate and Ultra Low Power WSN Node", 2013.

[3] G. Yue, Y. Xie, and H. Wen, "*The security issue of WSN based on cloud computing for smart grid*," Information Technology, vol. 12, no. 22, pp. 6702–6709, 2013. https://doi.org/10.3923/itj.2013.6702.6709.

[4] M. Sajid, K. Khan, U. Qasim, Z. A. Khan, S. Tariq, and N. Javaid, "*A New Linear Cluster Handling (LCH) Technique Towards Energy Efficiency in Linear WSNs*," 2015 IEEE 29th International Conference on Advance Information Networking and Applications (AINA), vol. 7, pp. 389–393, 2015.

[5] M. Rezaeirad, M. Orooji, S. Mazloom, D. Perkins, and M. Bayoumi, "*A novel clustering paradigm for key pre-distribution: Toward a better security in homogenous WSNs*," 2013 IEEE 10th Consumer Communication Networking Conference (CCNC), pp. 308–316, 2013. https://doi.org/10.1109/CCNC.2013.6488463.

[6] S. M. Sakharkar, R. S. Mangrulkar, and M. Atique, "*A survey: A secure routing method for detecting false reports and gray-hole attacks along with Elliptic Curve Cryptography in wireless sensor networks*," 2014 IEEE Students' Conference Electrical Electronic Computer Science, pp. 1–5, 2014.

[7] Q. Zhao and Y. Nakamoto, "*Routing Algorithms for Preventing Energy Holes and Improving Fault Tolerance in Wireless Sensor Networks*," Proc. 2nd International Symposium *on* Network Computing, pp. 278–283, 2014. https://doi.org/10.1109/CANDAR.2014.18.

[8] K. Y. S. B and S. S. Tyagi, "*SAERP : An Energy Efficiency Real-time Routing Protocol in Wireless Sensor Networks*," pp. 249–254, 2014.

[9] M. R. Ahmed and D. Sharma, "*Protecting wireless sensor networks from internal attacks based on uncertain decisions*," 2013 IEEE Wireless Communication Network Conference, pp. 1854–1859, 2013.

[10] Deepali and Padmavati, "*Improved energy efficiency semi static routing algorithm using sink mobility for WSNs*," 2014 Recent Advance Engineering and Computational Sciences (RAECS).pp. 1–5, 2014.