IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Volume-5, Issue-6 E-ISSN: 2347-2693

Game Theory Based Security Approach in Wireless Sensor Network

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

[1*] Department of Computer Science, Bharathiar University, Coimbatore, India
[2]Department of MCA, Muthayammal Engineering College, Rasipuram, Nammakkal, India

**Corresponding Author: murugandbc1976@gmail.com, Tel.: +919842636119*

Available online at: www.ijcseonline.org

Received: 09/May/2017, Revised: 16/May/2017, Accepted: 14/Jun/2017, Published: 30/Jun/2017

***Abstract*—** Wireless sensor networks have gone through a lot of changes in recent years. Secrecy in data transmission and network standby time are a major concern in communication. Currently, DSR algorithm is used for transmission of data between nodes. The algorithm determines the path for data to be transmitted to the destination node. Once the path is determined, all data are transmitted through the path. This method of data transmission drains the battery of the nodes quickly when the nodes are stationary. All the data are transmitted in a single stretch through the data path selected. When someone gains access to this path, all the data can be collected, and the entire network is compromised. A theory is implemented for eliminating this game. The data path is selected such that the battery level of all the nodes is effectively used. The data are spit and transmitted using more than one path for enhancing data security.

***Keywords*—** Network Life Time, Data Encryption, Game Theory.

I. INTRODUCTION

Wireless sensor network is implemented in all areas for collection of data. Data security and network lifetime are the vital parameters when it comes to selecting the algorithm for a particular application. DSR algorithm is currently used for transmission of data between the nodes. The algorithm works such that without any consideration to node's battery level the shortest path is selected to transmit data between the nodes. This is a major problem when the nodes are stationary. This is so because the shortest path in stationary nodes will be the same until a node in the middle goes off. This continued transmission will not efficiently use the energy level of all the nodes in the network. So, game theory is introduced for this purpose. An aloof, remote sensor arranges in the light of the Surface Acoustic Wave (SAW) resonators. The sensor hub comprises the SAW sensor that is little, light, solid, steady, delicate, remote and aloof, making the battery unnecessary, and its life-range is unending. The sink hub accumulates information from the sensor hubs, forms the information with clever calculations and transmits the required information to the system opportune outside. The essential structure and the acknowledgment of the inactive remote sensor system are expounded. The five fundamental qualities of the detached, remote sensor arranges are inactive sensor hubs, basic and little sensor hubs, sorted out sensor hubs, wise sink hubs, high security, great extendibility, with solid classification. Uniquely, the key methods in our examination, for example, coding and deciphering systems of the sensor hub, signal recurrence estimation procedures of the sensor hub, keen flag preparing strategies, estimation blunder remuneration systems, and system security systems, from the subject matter of an extensive and through discussion. At last, we call attention to the issues at present and figure the application prospect and research heading later on [1].

Remote sensor organizes hubs arrangement enhancement issue is examined with the remote sensor hubs organization deciding its ability and lifetime. A heterogeneous remote sensor organizes hubs organization calculation taking into account the apparent likelihood show going for the heterogeneous remote sensor arrange hubs which are arbitrary conveyed is composed in this article. The apparent likelihood model is utilized to ascertain the apparent likelihood in the zone around the heterogeneous remote sensor hubs and change virtual drive calculation. The calculation moves the heterogeneous remote sensor hubs to the low saw likelihood range and accomplishes the greatest scope of the checking zone. The reproduction that comes about demonstrates the accomplishment of this organization calculation in the objective of the hubs sensible dissemination with enhancing the system scope impact and decreasing the hubs development removing and augmenting the lifetime of heterogeneous remote sensor arrange later [2].

II. RELATED WORK

The proposed remote sensor framework, which comprises various leveled sensor organization and an application

system, empowers the use of pervasive processing. The progressive sensor organizes 1) a sensor system, where groups of sensor hubs impart using IEEE 802.15.4 to a sink hub 2) a hand-off system, comprising of Wideband Relay Nodes (WRNs). The WRNs go about as IEEE 802.11 b/g. The applications arrange utilizes the same radio channel as the hand-off system. This paper portrays the analyzes and re-enactments of the remote sensor framework. We suggest that IEEE 802.15.4 and IEEE 802.11 b/g utilize the same direct in the 2.4 GHz band, and, propose controlling activity of IEEE 802.11b/g later, changing IEEE 802.11 b/g MAC convention keeping in mind the end goal to forestall inter-channel impedance between IEEE 802.15.4 and IEEE 802.11 b/g. Our tests and re-enactments demonstrate the capability of two distinctive system frameworks working in the same recurrence channel: the progressive sensor arranges, and the application organizes [3].

The vitality of sensor hubs is a rare asset in remote sensor organizes. It is indispensable for reducing the vitality utilization to enhance the lifetime of remote sensor organizes. A capable approach to enhance lifetime is to segment sensor arrange into gatherings called bunch with high vitality hub going about as pioneer of the group called bunch head. Bunch head is in charge of overseeing intra-group and entomb group correspondence. The vitality level of group head at a given purpose of time decides the life of bunch and in this way entire sensor organizes. Disappointment in the bunch head conveys group correspondence to the end and may require re-grouping for getting sensor organizes back on track. These exercises include extra vitality use and, at last, have an extraordinary effect on the lifetime of the sensor system in the entirety. This paper proposes to have a group of bunch heads inside of the group of sensor hubs for adjusting the vitality utilization among the bunch heads. Given a minute, one bunch head goes about as ace of the given group and the ace ship is pivoted among group heads after the indicated number of adjusts of correspondence. This enhances the vitality use of sensor system, augments the system lifetime and makes the remote sensor organize blame tolerant to some degree [4].

Appropriate data deduction in remote sensor systems is of great significance for some true applications in which graphical display of a sent remote sensor system is the key. One basic issue confronted today is the way to take in the graphical model parameters of a sent sensor arrange as proficiently as could be expected under the circumstances since it is normally costly or even difficult to gather a lot of preparing information in a conveyed remote sensor organize given the asset limitations of modest remote bits. This paper endeavors to address this issue. We propose a novel portion based approach in graphical model learning for remote sensor systems to minimize the number of preparing tests of genuine sensor information required. We indicate the proposed approach by reproductions utilizing true remote sensor organize information. Our outcomes demonstrate the probability of the proposed part based learning approach significantly diminishing the volume of preparing information required for building a Markov arbitrary field model of the sensor organize in contrast with the conventional learning approach without influencing the developed model's execution in conveyed data deduction [5].

Information security in remote sensor arranges incorporation of information validness, information privacy, and information accessibility. Giving attractive information security in remote sensor systems is a testing process since remote sensor arranges comprise a huge number of sensor hubs that are for the most part put in antagonistic or unattended situations which might be presented to a few assaults. Assaults incorporate Denial of administration assaults, due to hub trade off for example, particular sending assaults and report interruption assaults. The existing security outlines give just jump bounce security, and this jump bounces security functions admirably while expecting a uniform remote correspondence design. Hub to sink correspondence is the prevailing correspondence design in remote sensor systems and bounce jump security plan is not adequate in view of its presentation to a few assaults due to hub trade off. In the proposed work, mystery keys are bound to geographic areas and every hub store keys taking their area into account. This area mindful property confines the effect of traded off hubs without influencing end-end security. Secret keys are produced taking into account their area and utilizing RSA calculation encryption, while decoding is finished information classification. The proposed multifunctional key administration system guarantees both hub to-sink and hub-to-hub validation along the report sending courses. Additionally, the proposed information conveyance approach ensures effective in transit false information sifting and is exceptionally hearty against DoS assaults. The assessment shows that the proposed plan is profoundly strong against an expanding number of traded off hubs and compelling in vitality investment funds [6].

Remote sensor systems are another sort of organized frameworks, described by seriously obliged computational and vitality assets, and a specially appointed operational environment. Since sensor systems may collaborate with delicate information and work in threatening unattended situations, it is basic that these security concerns be tended to form the earliest starting point of the framework outline. Be that as it may, security in sensor arranges postures diverse difficulties than conventional system security due to natural asset and processing requirements. There is presently huge research potential in the field of remote sensor arrange security. In this paper, we present a message expansion issue which can be settled by an information interface layer security design called dasiaCipher-content Stealing

methodpsila for remote sensor arranges. Customary security conventions have a tendency to be a traditionalist in their security ensures, regularly including 16-32 bytes of overhead. With little recollections, powerless processors, restricted vitality, and 30-byte parcels, sensor arranges cannot manage the cost of this extravagance. TinySec addresses these amazing asset imperatives with a cautious outline. We investigate the tradeoffs among various cryptographic primitives and utilize the innate sensor organize impediments further bolstering our good fortune while picking parameters for locating a sweet spot for security, parcel overhead, and asset necessities [7].

The measure of information transmission has turned into a critical issue in WSN. The innovation of compressive detecting (CS) in sensor organizes new thought for information gathering and target restriction as research regions in sensor arranges. Compressive Sensing (CS) minimizes the quantity of information transmissions and adjusts the movement stack all through systems. After all, by utilizing immaculate compressive detecting, the aggregate number of transmissions for information gathering is still high. Cross breed strategy for Compressive Sensing (CS) is utilized for minimizing the quality of transmission in sensor organizes. Further to give information pressure in WSN a light weight Enhanced Lossless Entropy Compression (LEC) calculation is utilized for abvidgency the size of information in the Sensor Network. Security is the significant issue in the Sensor Network and identity SET-IBS convention is utilized for making the information secure and for efficient transmission. It is a light weight calculation which consumes less vitality while scrambling and unscrambling the information. This encryption takes less vitality and it is useful to make the WSN proficient along these lines. In this anticipate the fundamental center is on the improvement of vitality as far as lightweight security and pressure procedures which diminish the multifaceted nature of Wireless Sensor Network the Advance SET-IBS convention for encoding the information on the sensor hub is proposed [8].

Remote sensor organizes (WSN) comprises independent sensor hubs appended to one or base stations. One of the primary objectives of remote sensor systems is to convey dependable data starting with one hub then onto the next hub in a system. As Wireless sensor organizes keep on developing, they get to be helpless against assaults and consequently the requirement for powerful security instruments. Distinguishing proof of suitable cryptography for remote sensor systems is a vital test due to restriction in vitality, calculation ability and capacity assets of the sensor hubs. In this paper we have executed Encryption calculation AES (Advanced Encryption Standard) to give adequate levels of security to ensuring the secrecy of the information in the WSN arrange [9].

Remote Sensor Networks have been a noteworthy region in the exploration of Security Authentication and the Data Access Control. This paper exhibits a conveyed information meant to control conspire fine-grained get to control over sensor information which is safe against solid assaults, for example, sensor trade off and client plotting. Here another security component is proposed in the characterized grouping construction which incorporates base station, bunch heads, and the sensor hubs. The information is transmitted utilizing the group head rather than direct transmission from individual sensor hubs to the base station and in this way, the vitality rationed for the sensor hubs are abundantly decreased preparing for long time information transmission. Disseminated Cluster Heads and Base station are composed utilizing the NS2 Simulation Environment. The proposed conspire misuses an Advanced Encryption Standard (AES) with CCMP (CBC-MAC), which ad libs, adjusts and balances out the WSNs as for both execution and security necessities. This paper gives understanding and change to acknowledge circulated fine-grained information get to control in grouped environment and the symmetric encoded systems utilizing AES with CCMP [10].

III. METHODOLOGY

Game theory is used for selecting the optimal path for data transmission. This optimal path is determined by the battery level of all nodes in the network. Data security is also addressed in the game theory. The optimal path is selected ensuring collection of the battery level of all nodes, and the data is transmitted through nodes that have more energy in the network. This method improves the network life of the entire network. To enhance data security, the data's are not only transmitted by a single path. Instead, the entire data block is split into blocks. More than one data path is determined, and each block is transmitted through a different data path. If a hacker gains access to a particular data path, only the block of data is accessible. By monitoring the unusual activity in the network traffic, the compromised nature or otherwise of the node can be determined. The network life time and data security are enhanced through the use of the game theory.

IV. RESULTS AND DISCUSSION

The algorithm is implemented in network simulator (ns2) for validating the effects of the game theory. Initially the nodes are created as shown in Figure 1.

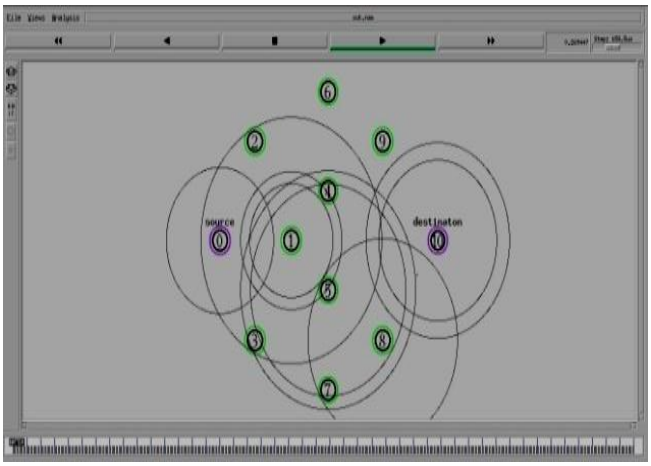

Figure 1. Node creation

The data transmission is started between nodes. The optimal data paths are selected, and each block of data is transmitted between nodes. The throughput and network life time of the entire network are increased through implementation of this algorithm compared to the network which works on DSR algorithm.

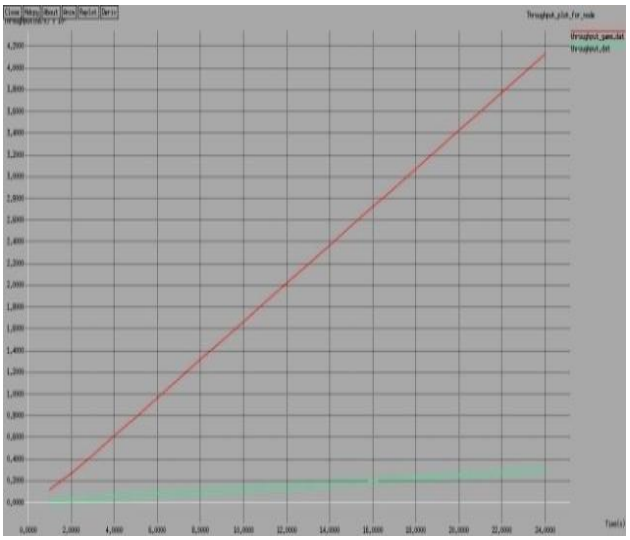

Figure 2. Throughput

Figure 2 shows the comparison of throughput between the networks working on the different algorithm.

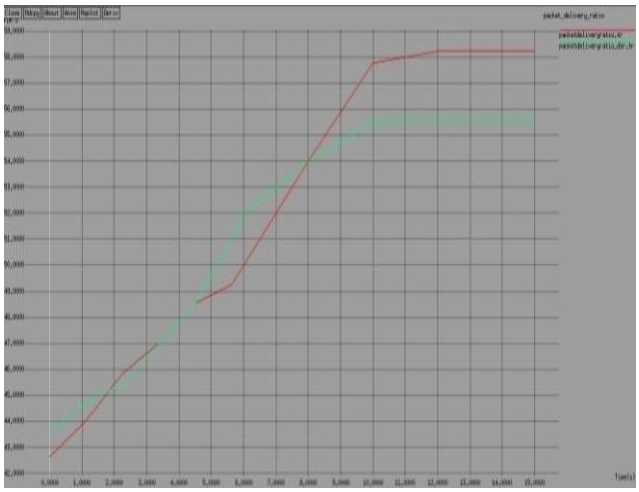

Figure 3. Packet Delivery Ratio

The packet delivery ratio of the network working under game theory algorithm is more than that compared to network working under DSR algorithm.

V. CONCLUSION

The main conclusions of the study may be presented in the above discussion clearly shows that game theory algorithm utilizes the energy in the network effectively more than DSR algorithm. Secrecy in data transmission is also more compared to DSR algorithm. The proposed method is implemented on ns2 to validate our claim.

REFERENCES

[1] Xiangwen Zhang; Fei-Yue Wang "*Key Technologies of Passive Wireless Sensor Networks Based on Surface Acoustic Wave Resonators*". Networking, Sensing and Control, IEEE International Conference (ICNSC) on 6-8 April 2008, pp. 1253 – 1258.

[2] Shi-Wei Li; Dong-Qian Ma; Qiang-Yi Li ; Ju-Wei Zhang; X. Zhang "*Nodes deployment algorithm based on perceived probability of heterogeneous wireless network*". International Conference on Advanced Mechatronic Systems (ICAMechS), 25 – 27 Sept. 2013 pp: 374 – 378.

[3] Keisuke Nakatsuka, Kenzo Nakamura, Yuichi Hirata, Takeshi Hattori "*A Proposal of the Co-existence MAC of IEEE 802.11b/g and 802.15.4 used for The Wireless Sensor Network*" 5th IEEE Conference on EXCO, Daegu, Korea October 22-25, 2006.

[4] Vaibhav V. Deshpande; Arvind R. Bhagat Patil "*Energy efficient clustering in Wireless Sensor Network using Cluster of Cluster heads",* Wireless and Optical Communication Networks (WOCN), 2013, Tenth International IEEE Conference on 26 – 28 July 2013, pp: 1 – 5.

[5] Wei. Zhao; Yao. Liang "*Kernel-based Markov random fields learning for wireless sensor networks*", Local Computer Networks (LCN) IEEE 36th Conference on 4 -7 Oct 2011, pp: 155 – 158.

[6] M. Jeyalakshmi "*Location aware end-end data security using Mac for secured wireless sensor networks*". International Conference on Advances in Engineering, Science, and Management (ICAESM), 2012.

[7] Md. Anisur Rahman, Mitu Kumar Debnath "*An energy-efficient data security system for Wireless Sensor Network*", 11th International IEEE Conference on Computer and Information Technology, (ICCIT) 24 – 27 Dec. 2008, pp: 381 – 386.

[8] Akshay S. Nagdive, Piyush K. Ingole "*An implementation of energy efficient data compression & security mechanism in* clustered Wireless Sensor Network", International IEEE Conference on Advances in Computer Engineering and Applications (ICACEA), 19 – 20 March 2015, pp: 375 – 380.

[9] M. Panda "*Data Security in Wireless Sensor Networks via AES algorithm*". IEEE 9th International Conference on Intelligent Systems and Control (ISCO), 9 – 10 Jan. 2015. pp: 1 – 5.

[10] R. Velayutham, J. Mary Suganya "*Security Authentication through AES and fine-grained distributed Data Access Control using Clustering in Wireless Sensor Networks*". Third International Conference on Computing Communication and Networking Technologies, 26 – 28 July 2012, pp: 1- 6.

Authors Profile

A. Muruganandam, Asst. Professor cum Head, Department of Computer Science, Don Bosco College, Adhiyaman Bye Road, Dharmapuri, Tamilnadu, India. He is a Research Scholar in the field of Wireless Sensor Networks at Bharathiyar University, Coimbatore, Tamilnadu, (India). His research is focusing on Secure Data for preventive and selective jamming attacks in Wireless Sensor Network. He has 15 years of teaching experience and 5 years of Research Experience.

Dr. R. Anitha is currently working as Professor & Director in the Department of Master of Computer Applications, Muthayammal Engineering College, Rasipuram, Tamilnadu, India. She has obtained her MCA Degree from Bharathidasan University, Tiruchirappalli, and Ph.D. from Periyar University, Salem. She has vast experience in teaching as well as research. She has presented papers at several International and National Conferences and has published research articles in leading Journals. She is an active researcher and is usually associated with reputed Academic Forums and Associations of research interest.

