iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 5 **Issue:** VII **Month of publication:** July 2017

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 5 Issue VII, July 2017- Available at www.ijraset.com

A Study of Game Theory Approach used for WSNs

Abhijit M. Mandape[1], Mrs. Sayali N. Mane[2]
[1,2]*Communication Network, Dept. of E&TC, D. Y. Patil College of Engineering*

Abstract: ***WSN security and its performance has been a major challenge since their application in various areas has grown. The application varies from security, medical, military and multiple more applications, also the WSNs have become an integral part of our daily lives. As a result, it becomes mandatory to employ techniques to assess the need of security and performance needs of WSN. Game theory holds a prospective approach and solution towards the security and performance needs of the WSNs. In the paper, we study the Game theory and also discuss work in which Game Theory is used for tackling the issues that occur in the WSNs.***

Keywords: WSNs, Game Theory, NASH Equilibrium, Trust derivation, Security.

I. INTRODUCTION

Game theory is a branch of mathematics that can be used to analyze system operations in decentralized and self-organizing networks also describe and analyzes interactive decision situations. Game theory has been under deployment throughout the history [1]-[2]. John von Neumann and Oskar Morgenstern invented the mathematical theory of games in the year (1944). Despite the fact that the theory has been used mathematically and logically systematic only since 1944, game-theoretic insights can be found among commentators going back to pre-historic times. For example, in Plato's writings, the *Laches* and the *Symposium*, Socrates remembers an episode from the Battle of Delium that some commentators have interpreted as involving the following situation. Let us consider a soldier at the front, waiting with his comrades to drive back an enemy attack. It may occur to him that if the defense is likely to be successful, then it isn't very probable that his own personal contribution will be important. But if he stays, he runs the risk of being wounded or killed—apparently for reason. On the other hand, if the enemy is going to win the battle, then his chances of death or injury are higher still, and now quite clearly to no point, as the line will be overwhelmed anyway. Based on this reasoning, it would appear that the soldier is better off running away regardless of who is going to win the battle. Of course, if all of the soldiers will reason this way—as they all apparently *should*, since they're all in similar situations—then this will certainly *bring about* the outcome in which the battle is lost. Of course, this point, since it has occurred to us as predictors, can occur even to the soldiers. Does this give them a valid reason for staying at their posts? On the other hand: the greater the fear of the soldiers for the battle will be lost, the greater their enticement to get themselves out of harm's way. And the greater the soldiers' belief that the battle will be won, without the need of any particular individual's contributions, the less reason they have to stay and fight. Soldier *anticipates* this sort of reasoning on the part of the others, all will quickly reason themselves into a panic, and their horrified commander will have a rout on his hands before the enemy has fired a shot. The ideas behind It provides logical tools to predict the result of complex interactions among logical entities, where rationality demands strict unity to a strategy based on perceived or obtained results.[4] The foundation of modern game theory can be considered as an extension of a three combined works; a "Researches into the Mathematical Principles of the Theory of Wealth" in the year 1838 by Augustine Carnot, gives an intuitive explanation of what would eventually be formalized as Nash equilibrium and gives a dynamic idea of players best-response to the actions of others in the game. In 1881, Francis Y. Ed the main areas of application of game theory are political science, economics, sociology and biology. In addition, it is today established throughout both the social sciences a wide and range of other sciences like Military etc.

II. GAME THEORY

Game theory, well-defined in the vast sense, is a pool of mathematical models catalogued to study events of conflict and cooperation. It is concerned with finding the best actions for individual decision makers in these situations and becoming aware stable outcomes. Let us consider a game in the following situation:

A. There are minimum two players: A player can be an individual, a company, a nation, a wireless node, or even a biological species.

B. The tact chosen by each player determine the result of the game.

C. Associated with each possible outcome of the game is a collection of numerical payoffs, one to each player. These payoffs represent the value of the outcome to the different players. In 1950, John Nash demonstrated that finite games have always have

an equilibrium point, at which all players choose actions which are best for them given their opponents' choices. [4] Nash equilibrium is a list of strategies, one for each player, which has the property that no player can unilaterally change his/her strategy and get a better payoff.[3] This central concept of non-cooperative game theory has been a focal point of analysis since then.

III. TERMINOLOGIES USED IN GAME THEORY

There are different terminologies used in a game theory and they are as follows:

A. Players

A strategic decision maker within the context of the game. Each participant is a player. There are two players in a game. The players maybe any two companies (for e.g. Company A and company B) competing for tenders, two countries were planning for trade gains in a third country, two persons bidding in a game, etc.

B. Strategy

The strategy of a player is the predefined rule by which a player decides his course of action from the list of courses of action during the game. In a game in strategic form, a strategy is one of the given possible actions of a player. In an extensive game, a strategy is a complete plan of choices, one for each decision point of the player. The strategy is of two types: pure and mixed strategy. Let m be the number of strategies of player A and n be the number of strategies of player B, p_i be the probability of selection of the alternative i of player A, i = 1,2,3,….m. Let q_j be the probability of selection of the alternative j of player B, for j = 1, 2, 3…..n. The sum of the probabilities of selection of various alternatives of each of the players is equal to 1 as shown below.

$$\sum_{i=1}^{m} p_i = 1 \;\&\; \sum_{j=1}^{n} q_i = 1$$

1) *Pure Strategy:* If a player selects a particular strategy with a probability of 1, then that strategy is known as a pure strategy. This means that the player is selecting that particular strategy alone ignoring his remaining strategies. If player A follows a pure strategy, then only one of the p_i values will be equal to 1 and the remaining p_i values will be equal to 0. A sample set of probabilities of selection of the alternatives for player A is shown below: The sum of these probabilities 0 p_3 1 p_2 0 p_1 is equal to 1.That is

$$p_1 + p_2 + p_3 = 0+1+0=1.$$

2) *Mixed Strategy:* If a player follows more than one strategy then the player is said to follow a mixed strategy. But the probability of selection of the individual strategies will be less than one and their sum will be equal to one. It is clear that the sum of the probabilities is equal to 1. That is

$$q_1+q_2+q_3=0.65+0+0.35=1$$

C. Payoff Matrix

The outcome of the game is called payoff. Payoff matrix is a table showing the outcomes or payoffs of different strategies of the game. When the outcome is random, payoffs are usually weighted with their probabilities. The expected payoff incorporates the player's attitude towards risk [3].

D. Actions

The choices made by a player are called action. The type of action taken determines the final outcome of a game.

E. Strategies

A particular plan of action that is taken for every contingency played by other players.

F. Rationality

A player in the game is called rational if he plays in such a way that his payoff increases.

G. Saddle Point

If in a game, the maximum value is equal to the minimum value then it is called at saddle point.

H. Value of the game

If the game has a saddle point, then the value of the cell at the saddle point is called the value of the game. [3]

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 5 Issue VII, July 2017- Available at www.ijraset.com

IV. WIRELESS SENSOR NETWORKS

Wireless Sensor Networks (WSNs) are comprised of multiple sensors which are connected to each other in order to perform collaborative or cooperative functions. WSN may have many cheap wireless sensor nodes, each with a capability of collecting, processing environmental information, , storing and communicating with neighboring nodes for exchange of information. WSN used in wide range of applications related to military and civil applications such as target field imaging, intrusion detection, weather monitoring, security and tactical surveillance, distributed computing, detecting ambient conditions like temperature, movement, sound, light, or the presence of certain objects, inventory control, and disaster management.[3] With the recent advancements in wireless communications sensor technology, and embedded system, we witness a exponential growth in the number of sensing devices connected to the Internet.[4] The needs for mobility and convenience access also encourage the use of wireless for the Internet access. With these developments WSNs have become an attractive platform for many services. Despite the advancements in WSN development, there are still a number of problems that remain unsolved in WSNs.

Wireless Sensor Networks (WSN) generally consists of multiple number of sensor nodes distributed over a certain location and the position of sensor nodes in not needed to be engineered or pre-determined. They transform data into electric signals, which are then processed to reveal some of the characteristics about the phenomena where it is located. The unique nature of the sensor networks is the cooperative effort of sensor nodes. Wireless sensor network can assist rescue operations by locating survivors, identifying risky areas, and making the rescue team more aware of the overall situation in a disaster area. The sensor nodes have the ability to communicate either among each other or directly to an external base station (BS). A larger number of sensors are used for sensing over large geographical regions with greater accuracy. The wireless sensor nodes are the central element in a wireless sensor network. Figure 1 shows the basic wireless sensor nodes deployment

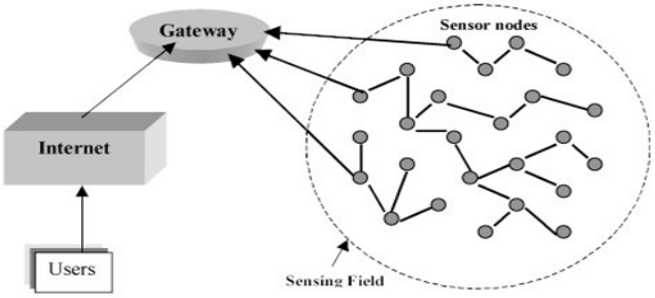


Fig. 1 Communication Architecture of Sensor Network

The most common WSN architecture follows the OSI architecture Model. The architecture of the WSN includes five layers and three cross layers. Mostly in sensor n/w we require five layers, namely application, transport, n/w, data link & physical layer. The three cross planes are namely power management, mobility management, and task management. These layers of the WSN are used to accomplish the n/w and make the sensors work together in order to raise the complete efficiency of the network.

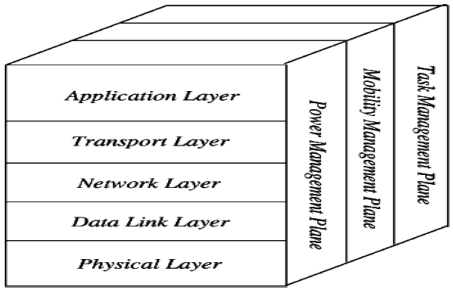


Fig. 2 Wireless Sensor Network Architecture

The physical layer provides an edge for transferring a stream of bits above physical medium. This layer is responsible for the selection of frequency, generation of a carrier frequency, signal detection, Modulation & data encryption. The choice of a good modulation scheme is critical for reliable communication in a sensor network. The data link layer is responsible for the multiplexing of data streams, data frame detection, medium access and error control. The Medium Access Control (MAC) protocol must be power-aware and able to minimize collision with neighbour's broadcasts. The network layer takes care of power efficiency of the node and route data supplied by the transport layer. The transport layer helps to maintain the flow of data if the sensor networks

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 5 Issue VII, July 2017- Available at www.ijraset.com

application requires it. This layer is especially needed when access to the system is planned through Internet or other external networks. Depending on the sensing tasks, different types of application software can be built and used on the application layer. In addition, the power, mobility, and task management planes monitor the power, movement, and task distribution among the sensor nodes. These planes help the sensor nodes to coordinate the sensing task and reduce the overall power consumption.

V. WSN SECURITY AND GAME THEORY

Identification of malicious nodes plays an important role in enhancing network security and performance. Various methods have been proposed to detect malicious nodes. These methods include monitoring the behavior of neighbors [6], weighing a node's behavior and measuring confidence based on the weight [7], using the sequential hypothesis testing to assess nodes' reaction [8], and using the activity records gathered by neighbours in different times [9]. Games Theory is another powerful method used by many researchers to identify malicious nodes or encourage collaboration with other participants. In reference [10], Gharaee et al. have proposed a strategy based on the Games Theory to provide a way in order to encourage malicious nodes to cooperate with others in heterogeneous wireless sensor networks. In references [11, 12], a method based on Bayesian game theory is suggested to model the interaction of malicious and normal nodes in order to identify malicious nodes and to understand how they act against being detected. The other method proposed in this field [13] is based on Bayesian game theory that tries to save energy. Bayesian game refers to a game, with incomplete information and different types of players. In this game, each player's action depends on the opponents' previous action. The selected action is based on using a possibility value calculated at each step.

Game theory can be used to capture the type of conflict in WSNs security. The essence of the attack defend can be expressed by mutual strategies of interdependence. Thus, WSNs security can be modelled by at least two players interacting in an attempt to maximize their desired objectives. The attacker's decision strategies are closely related to those of the defendant and vice versa. Whether defensive strategy is effective will not only depend on the defender's own action but also depend on the attacker's strategy. Besides, game theory can be utilized to perform tactical analysis of the options of WSNs threats produced either by a single attacker or by an organized group. It has the ability to examine the huge number of possible threat scenarios in WSNs. Game theory can also provide methods for suggesting several probable actions along with the predicted outcome to control future threats. Therefore, it is very profitable to employ the game theory to study the optimal attack and defence decision- making problems. Game theory is divided into two branches, called the non-cooperative and cooperative branches.

A. Cooperative Game Theory

A cooperative game is a game in which the players can make irrevocable commitments. Analysis in cooperative game theory is centred on union formation and distribution of wealth gained through cooperation within these two areas, finding procedures leading to outcomes that are most likely to occur under reasonable rationality assumptions in various game situations, and devising solution concepts showing attractive stability features are primary concerns in most research endeavours. Cooperative game theory is most naturally applied to situations arising in political science or international relations, where concepts like power are most important.

B. Non-Cooperative Game Theory

In no-cooperative game theory, the players do not form a coalition with each other as that in cooperative game theory and play the game with respect to their own self interest. As per the moves performed by the players, simultaneous or not, the non cooperative game is divided into two parts: Static and dynamic. In static game, players make their choices of strategies simultaneously. None of the player has any information about the strategy of another player. This strategy can be made in isolation, with no information what other player has done or will do, even if decision is made at other point of the game. This game can be diagrammatically represented using a game table called strategic table. In dynamic game players involve strategic situation which has a strict order of play. Players take turns to make their moves, and they know what strategy has been performed by the players who have gone before them. Dynamic games are most easily illustrated using game trees, which are generally referred to as the extensive form of a game. The trees illustrate all of the possible actions that can be taken by all of the players and also indicate all of the possible outcomes from the game. [4]

C. Characteristics of Game

There are multiple game theory models which can be place in groups on the basis of factors like the number of players involved in the game, the sum of gains or losses, the number of strategies employed in the game and it can be designed as a one-player game, two-player game or players game. The nomenclature used in game theory is inconsistent, thus different terms can be used for the

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 5 Issue VII, July 2017- Available at www.ijraset.com

same concept in different sources. The commonly used Game theory methods for solving WSN problems and several main terminologies are listed in Table 1.

Game Theory Methods	Common Terminologies in Game Theory
(i) Cooperative game theory	(i) Nash Equilibrium
(ii) Non cooperative game theory	(ii) Pareto Optimal
(iii) Repeated game theory	(iii) Nash Bargaining Solution
(iv)Coalitional game theory	(iv) Shapley Value
(v)Evolutionary game theory	(v) Core
(vi)Guar game theory	(vi) Mechanism Design (Computational)
(vii)Bargaining game theory	(vii)Incentive compatible
(viii)Dynamic game theory	(viii)Strategy proof Mechanism
(ix)TU game theory (transferable-utility game)	(vii) Auction
(x)NTU game theory(nontransferable-utility game)	(viii) Viceroy-Clarke-Groves(VCG) Mechanism
(xi)Ping-pong game	(ix) Utility Function
(xii)Zero-Sum game and NonZero-Sum game	(x) Bayesian Nash Equilibrium(BNE)
(xiii)Jamming game	

Table 1. Typical Game Theory methods and common terminologies of Game Theory used in Wireless Sensor Network.

VI. RELATED WORK

The works related to this paper, which are for WSNs, mainly include surveys on intrusion detection system, security, and game theory.

R. Machado and S. Tekinay[14], in their survey the use of concepts of game theory to solve the problems of energy efficiency, security, and detection and tracking in WSNs. They discuss the game-theoretic approaches in WSNs for energy efficiency in three aspects: energy conservation, routing, and load balancing. They consider three different security scenarios: intrusion detection, intrusion by injecting a malicious packet, and preventing the broadcast message by malicious sensor nodes. They also summarize recent research on pursuit-evasion game used to model detection, tracking and surveillance applications in WSNs.

E. Sabbah and K. Kang [15], discuss security challenges and vulnerabilities in WSNs. They survey representative security mechanisms designed to address known vulnerabilities and highlight key research issues that remain to be tackled.

Junqi Duan et.al., [16], In their paper propose a trust derivation scheme using prisoners dilemma game to detect and punish the malicious nodes. Using his approach they improve the energy and the ease of approach to detect the malicious nodes which are affecting the performance of the WSN environment.

Ritu and Pooja Alhawat [17], in their paper, a game theory adaptive model is defined to identify the safe communication path over the network. The presented model is divided in two main stages. A jamming attack is considered on the network. This attack occurs because of high communication in the network performed by internal network nodes. As the heavy communication increases the energy consumption and load in the network, the overall criticality of network also increases.

Y. Mao, P. Zhu, and G. Wei [18], in their paper, propose a method based on the game theory was introduced to detect malicious nodes in wireless sensor networks. In this method, it is assumed that the number of malicious nodes is much less than the number of normal nodes and each node is not aware of the other nodes' type. The purpose of this paper was to detect abnormal behavior of malicious nodes.

J. Chen et al.,[19] In their paper, provided a way to avoid dropping messages on P2P networks. The game presented in this paper is an iterative and two-player game between two neighboring nodes in the P2P network. In fact, the data exchanging between neighboring network nodes is modeled as a game. As a result, the game is iterative and will be presented at all stages of the network.

T. Alpcan and S. Buchegger [20], in their paper, proposed some methods based on game theory to maintain the security of mobile ad hoc network. These algorithms are designed for networks whose members adopt restrictions on the use of its resources. These algorithms cannot be used in networks whose members have a high degree of mobility without any restrictions.

X. Chen et al., [20], in their paper, identify the threats and vulnerabilities to WSNs and summarize the defense methods based on the network protocol layer's analysis. They divide these secure issues into seven categories: cryptography, key management, attack detections and preventions, secure routing, secure location security, secure data fusion, and other security issues. They also point out open research issues and directions in each category.

Considering some of the work mentioned in the paper on the application of game theory in the security of WSN's, it can be said that the game theory holds a very vast potential in the security and performance of WSN.

VII. CONCLUSION

Game theory is the study of how players should play games rationally, and it is a powerful tool in many areas, such as war, politics, economics, sociology, psychology, biology, and communications, networking and so on where the conflict and cooperation exist. WSNs security is a very important research area. Due to the constrained capabilities of sensor nodes, providing security to sensor networks is a challenging task, however, there are not popular applications of WSNs without considering WSNs security. Game theory has the capability to exam a larger amount of possible scenarios before performing the action. It can sophisticate a decision process as a modelling tool. The direction of applying game theory to WSNs security is prospective. Also there have been many researches in game theory for the application in the security and performance improvement of WSNs. The game theory is an effective tool to counter all the security needs and performance enhancement for the WSNs in present and future.

REFERENCES

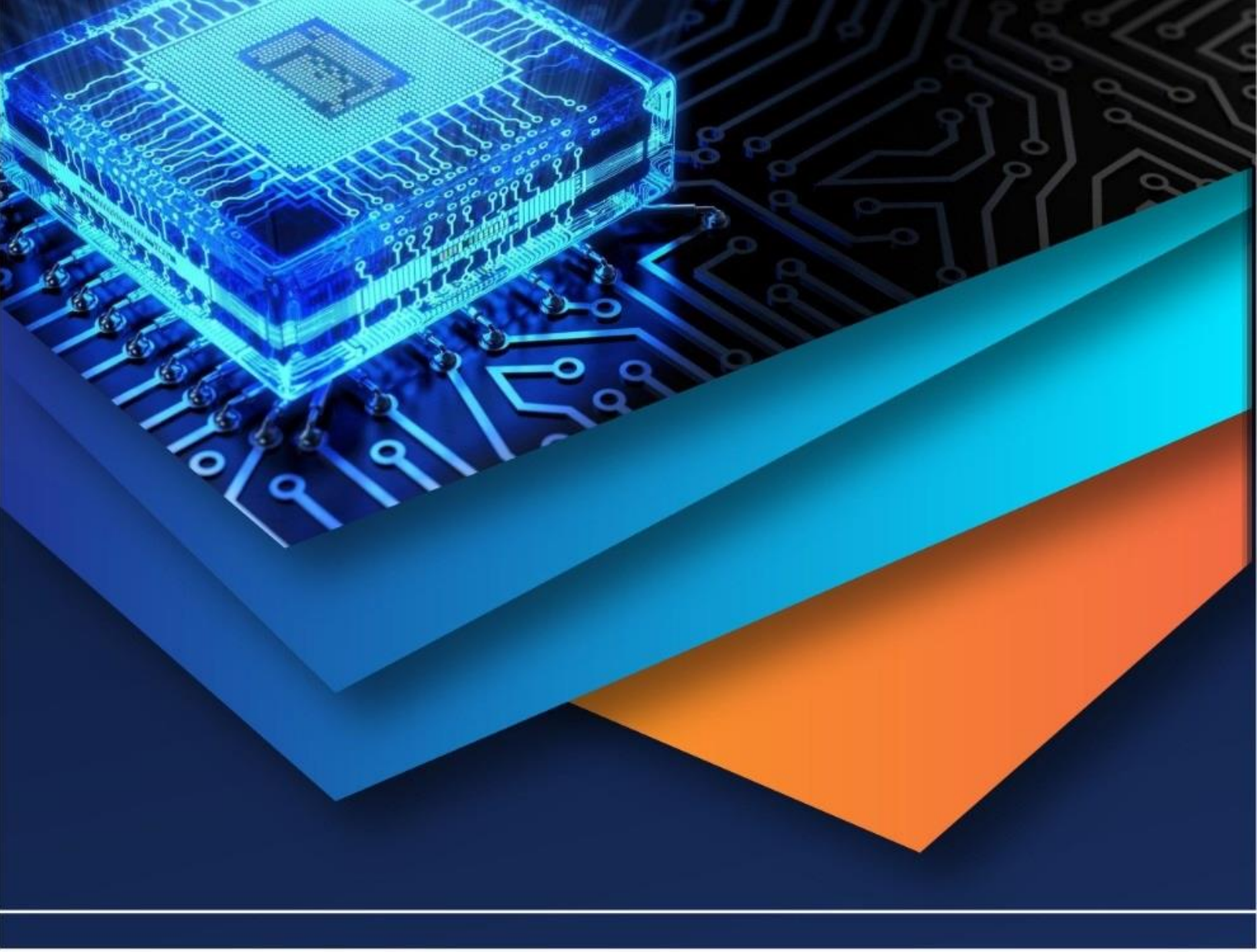
[1] Srivastava et al., "Using Game Theory to Analyze Wireless Ad Hoc Networks"
[2] Hai-Yan Shi, Wan-Liang Wang, Ngai-Ming Kwok and Sheng-Yong Chen , Sensors 2012, 12, 9055-9097; doi: 10.3390/s120709055
[3] Vinoba.V, Chithra.S.M "The Study of Game Theory in Wireless Sensor Networks" International Journal of Emerging Trends & Technology in Computer Science. Volume 3, Issue 5, September-October 2014.
[4] Theodore L. Turocy, Bernhard von Stengel "Game Theory" CDAM Research Report LSE-CDAM-2001-09, October 2001.
[5] Abhijit M. Mandape, Mrs. Sayali N. Mane "An Improved Energy Aware Trust Derivation Scheme" International Journal of Advance Research, Ideas and Innovations in Technology. Volume 3, Issue 1, 2017.
[6] S. Tomasin, "Consensus-based detection of malicious nodes in cooperative wireless networks," IEEE Communications and Letters, Vol. 15, 2011, pp. 404-406.
[7] O. Seo, H. Chan, O. Hong, and Y. Hwa Choi, "A malicious and malfunctioning node detection scheme for wireless sensor networks," Wireless Sensor Network, Vol. 4, 2012, pp. 84-90.
[8] H. Jun-Won, M. Wright, and S. Das, "Distributed detection of mobile malicious node attacks in wireless sensor networks," Ad Hoc Networks, Vol. 10, 2012, pp. 512- 523. 7.
[9] Y. Sung-Jib and Y. Choi, "Neighbor-based malicious node detection in wireless sensor networks," Wireless Sensor Network, Vol. 4, 2012, pp. 219-225. 8.
[10] M. Shamani, et al., "Adaptive energy aware cooperation strategy in heterogeneous multi-domain sensor networks," Procedia Computer Science, Vol. 19, 2013, pp. 1047-1052. 9.
[11] W. Wang et al., "A game theoretic approach to detect and co-exist with malicious nodes in wireless networks," Computer Networks, Vol. 71, 2014, pp. 63-83. 10. L.
[12] Feng, Y. Yang, and J. Wu, "Attack and flee: game-theory-based analysis on interactions among nodes in MANETs Systems," IEEE Transactions on Systems, Man, and Cybernetics, Part B: Cybernetics, Vol. 40, 2010, pp. 612-622. 11.
[13] J. Roles, H. Elaarag, and E. Friedman, "A Bayesian game approach to coexistence with malicious and selfish nodes in wireless ad-hoc networks," in Proceedings of the 17th Communications and Networking Simulation, 2014, pp. 50-57.
[14] R. Machado and S. Tekinay, "A survey of game-theoretic approaches in wireless sensor networks," Computer Networks, vol. 52, Nov. 2008, pp. 3047-3061

[15] E. Sabbah and K. Kang, "Security in wireless sensor networks," in Guide to Wireless Sensor Networks, S. C. Misra, I. Woungang, and S. Misra, Eds. Springer London, 2009, pp. 491-512

[16] Junqi Duan, Deyun Gao, Dong Yang, Chuan Heng Foh, Hsiao-Hwa Chen "An Energy-Aware Trust Derivation Scheme With Game Theoretic Approach in Wireless Sensor Networks for IoT Applications"

[17] Ritu, Pooja Alhawat "Game Theoretic Modeling of WSN Jamming Attack and Detection Mechanism" , International Journal of Computer Science and Mobile Computing, Vol.4 Issue.6, June- 2015, pg. 648-653

[18] Y. Mao, P. Zhu, and G. Wei, "A game theoretic model for wireless sensor networks with hidden-action attacks," International Journal of Distributed Sensor Networks, Vol. 2013, 2013, pp. 1-9



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY