ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)
Volume 2, Issue 6, June 2013

IMPLEMENTATION OF MOBILE TARGET DETECTION IN WIRELESS SENSOR NETWORKS

J.NAVEEN, S.MADHU PRIYA

***Abstract*—** Through wireless sensor networks, the surveillance applications are considered where has to choose one path between a set of candidate sites where to place sensors in order to identify mobile targets traversing a prearranged region. The existing system was designed with the intend of minimizing the sensor installation costs whereas promising that the spotlight of any path is above a definite threshold, and maximizing the coverage of the least uncovered paths subject to a resource on the sensors setting up charges. Through this motivation the Tabu Search heuristics are employed that are capable of endow with near-optimal resolutions of the same occurrences in tiny computing occasion in addition attempt huge size occurrences. The vital descriptions are widened to account for limitations on the wireless connectivity with assorted machines and non-uniform sensing. In this there can be an attacker may be able to capture and compromise mobile nodes, and then that can be utilized to insert bogus data, interrupt network functions, and eavesdrop on network communications. To defeat this problem a novel mobile replica detection system is suggested based on the Sequential Probability Ratio Test (SPRT). Here the intuition is exercised that an uncompromised mobile node ought to shift at speeds exceeding the system-configured maximum speed. If the outcome is observed that a mobile node's speed is in excess of the maximum speed, it is afterward extremely probable that in any case two nodes with the unchanged identity are present in the network. Particularly, the SPRT achieves on each mobile node via a null assumption that the mobile node hasn't been reproduced and an exchange hypothesis that it has. The proposed system is also developed to attain the goal of weighted intrusion detection,and maximizing the network using game theory approach,life time of the sensor node is increased. Above all, experimental results illustrate that proposed scheme very rapidly senses mobile replicas with zero false positive and negatives. This is essential since the SPRT is confirmed to be the paramount system in terms of the number of observations to achieve a decision between all sequential and non-sequential decision practices.

Keywords: Wireless Sensor Networks, Tabu Search Heuristics Method, Mobile Targets, Mobile Replica Detection, Sequential Probability Ratio Test, Mobile Target Detection, Optimization Resolutions, Game theory

.

***Manuscript received June, 2013*.**

J.Naveen, Computer Science, Anna University Chennai/ A.S.L Paul's College Of Engineering And Technology/. Coimbatore,India,9943014326

***S.Madhu Priya**, Anna University Chennai/ A.S.L Paul's College Of Engineering And Technology/). Coimbatore,India, 9944403072*

INTRODUCTION

One of the main applications of wireless sensor networks is the target or event detection/tracking. Whereas most of the preceding work has been on static sensor networks, B. Liu et.al [1] in recent times it has been exposed that the coverage of a sensor network can be enhanced by the use of mobility. Mobile robots prepared with sensors can be positioned for efficient coverage in case of monitoring in nature inaccessible or hazardous areas. In addition, if the target or event to be perceived through the sensor network is about time-critical nature, the coverage of the network should be adequately high to be able to react to the sensed event in an appropriate manner; for example wildfire observing or dynamism detection under ruins in case of an earthquake, where the urgent situation personnel work in opposition to the timer. Exclusively, regarded as the subsequent condition: specified a sensor network, how does one negotiate throughout the sensor field from one point to another such that the sensors have the least or the majority coverage of the traveled path. This referred to as the least-covered path dilemma, signifies the sensor network's worst-case coverage. Sensor networks are intended to watch the sensor field, and the least-covered path computes the capability to travel in the sensor field with not being exposed. Consequently, how one can intend the sensor network to exploit such least coverage turns into very important and has concerned important concentration in recent times [2], [6], [7].

Two well-liked techniques dealing this problem are the maximum breach path and the minimal exposure path. The maximum breach path problem looks forward to discover a path such that the path's maximum exposure to the sensors at some known point is reduced [7]. The minimal exposure path problem searches forward to discover a path between two given points such that the total exposure obtained from the sensors by traversing the path is reduced [7], [8]. By means of the minimal exposure path dilemma to assess a network is essential. Previously the minimal exposure path is recognized; the user can influence sensors in the network or add sensors to the network to enhance coverage. Still, with a centralized method to resolve the minimal exposure path denotes that the moved/added node's location must be reported to a central node or to each other node in the network. A single-point-of-failure trouble occurs if a central node is utilized; if the new data is disseminated to each other node in the network, the difficulty of energy utilization turns out to be more significant. Consequently, we present a localized minimal coverage path algorithm such that simply adjacent nodes have to be updated and path information can be considered on-line in an easier and more competent method.

Even as the least coverage problem receives the distrustful view of the sensor network design, related to real-time system intends based on worst-case implementation time analysis, that we call it as the maximal exposure path problem. A maximal exposure path is the path of subsequent which the total coverage to the sensors is exploited; specifically, the path that is best covered by the sensors. In general, there is a maximum length constriction on the maximal exposure path or a delay constriction that specifies how long the object can wait in the sensor field. Or else, one can keep moving devoid of getting the ending point or stay at a point with optimistic revelation eternally to build up unlimited coverage. Contrasting the least coverage problem, that calculates how well the sensor network monitors its situation, the maximal exposure difficulty, even if it can be deduced as the best case of coverage, discovers applications in the environment that can advantage from the positioned sensors. These applications include, for case, how to supervise for example collecting information from the sensors, the sensor network competently and how to obtain the most advantage, in relation to any predefined benefit function, from the sensors whereas traversing the sensor field. A more physical example of using the maximal exposure path to resolve the benefit of a sensor network is regarding a light-detecting network.

The perception of barrier coverage is established in [14]. An exciting algorithm to resolve whether a network affords barrier coverage is presented. A centralized, most favorable sleep-wake up algorithm for achieving global barrier coverage is suggested in [15]. The notion of local barrier coverage is projected in [11]. This new notion of barrier coverage is basically more interesting than the original barrier coverage, and it facilitates the authors of [11] to enlarge localized sleep-wake up algorithms that affords near-optimal performance, even as ensuring global barrier coverage usually. The dilemma of deriving a dependable approximation for ensuring 1-barrier coverage in a random deployment is resolved in [9]. Several articles have conferred the difficulty of total sensors to an obtainable operation to attain a variety of properties, typically k-connectivity. In [10], an algorithm is projected that calculates the minimum number of extra sensors wanted to construct a sensor network k-connected. The excellence of k-connectivity measured there is either 1 or 0, which is \yes, it is k-connected" or \no, it is not." The metric of k redundancy is initiated in [16] to compute the local quality of k-connectivity; extra nodes (robots) are additional to expanses with low redundancy. Our work splits with [16] a similar support of measuring local excellence and recognizing areas that require repair.

Schillings and Yang et.al [20] utilized the GT framework to construct a query-based Versatile Game Theoretic Routing Protocol (VGTR) to achieve the extraction of data from WSN. Three payoff functions are exercised. The first two represent node survivability and the third one corresponds to the importance of the information collected. Node survivability signifies the competence of a node to continue in contact with the Sink for given that possible. To make clear these three payoff functions obviously, several definitions were utilized, for example Upstream Potential Path Nodes (UPPN) Robustness, and Neighbor Robustness. Affecting goals can be measured as intelligent agents and this characteristic frequently augments the tracking complexity. Conversely, sensor nodes only have limited wireless communication competence. Consequently, there is a want to discover a way to cooperate proficiently in target assessment. Gu et.al [21] applied a zero-sum game approach to the estimation of target position. The minimax filter is assembled to reduce the opinion error under the worst case noise; as a result it is robust to the adversary tracking complexity obligatory by moving targets. The work also developed a dispersed version of the minimax filter with an enhanced routine.

In our advance, we believe two main objects: minimizing the number of nodes positioned and maximizing the revelation of the least-exposed path. Given these complementary purposes, we suggest and examine two WSN planning dilemmas. In the first one, sensors must be situated with the intention of exploiting the coverage of the least-exposed path, because of experience resources on the installation cost with the number of sensors also the size of the sensors is reduced. In the second one, sensors have to be situated in order to diminish the mechanism cost, offered that the revelation of the least-exposed path is above a given threshold. The game theory is integrated to examine the coverage difficulties in Wireless Sensor Networks (WSN) in this manuscript. GCC (Game-theoretical Complete Coverage) algorithm is utilized to guarantee whole network coverage essentially from side to side regulating the covering range of nodes and calculating the network redundancy. After this, by scheming appropriate cost and usefulness function for every node, simulations establish the competence and applicability of GCC algorithm and also motivate that GCC is an outstanding way for time scheduling and maintenance Network Integrity.

The remainder of the paper is discussed as follows: Section 2 describes the previous work and the methods are explained. Section 3 deals with the proposed work and algorithm. In section 4 the results of the approach are explained and the comparison results are described. The conclusion and future of the work are explained in section 5.

PREVIOUS WORK

The concept of exposure [25] has been initiated to give a quantitative measure of the excellence of WSNs for the recognition of mobile objects traversing areas of concentration along a given path. Instinctively, the more depiction a path is, the better the coverage offered by the WSN, and the higher the probability to notice the mobile object touching along that path. The formal definition of experience perceptibly depends on the specific sensing model accepted and the way in which sensed data are utilized for discovery. A common sensing model presumes that the sensing machine is based on the energy of a signal established from the purpose that is the signal can be either produced or just reflected by the target [17]. Given a location p in the monitored area, the energy of the signal expected by a sensor at position s from a target in p is $I_s(p) = \frac{\lambda}{[d(p,s)]^{\gamma}}$, where $d(p,s)$ is the geometric distance between locations p and s, λ, is the energy emitted by the target, and γ is an energy decay factor. Since the exposure value of the least-exposed path is a measure of the vulnerability level of the network, maximizing this value is one of the objectives of the network planning problem. Clearly, another objective is to minimize the installation cost, which is directly related to the number of sensors deployed.

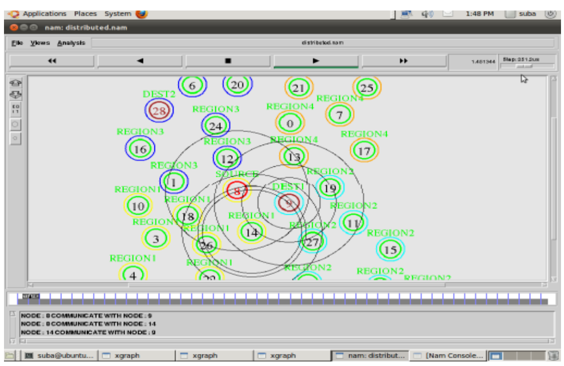

Fig 1: Distributed Wireless Sensor Network Environment

Thus, we address two versions of the problem: maximizing the exposure of the least-exposed path subject to a budget constraint on the cost, and minimizing the installation cost while guaranteeing that all paths have an exposure value above a given threshold. It is worth pointing out that the two versions deriving from the two contrasting objectives differ substantially. Note that the budget constraint is not tight in the exposure maximization problem. This leads to different duality properties, requires changes in the design of the related heuristics, and implies higher solution times. By adding constraints to these two basic versions, we can easily ensure wireless communications among the sensors. Given a sensor layout (a set of sensors located in a subset of candidate sites (CSs)) and their transmission ranges, consider the communication graph where sensors are connected by a link if they are in range. An additional node of the graph represents the sink device where all data must be delivered. To guarantee communication, a sensor layout must correspond to a connected communication graph. To account for resiliency to failures, we may require k-connectivity. Based on the same graph, we can also include capacity constraints on the node traffic, corresponding to limited transmission rates on the radio channel and/or to energy consumption limitations. Moreover, practical surveillance systems may integrate multiple types of sensing devices running different sensing technologies, with different capability/accuracy, as well as different installation costs. To this extent, we show how the basic optimization formulation can be extended to plan such heterogeneous systems, capturing further degrees of freedom.

Given the area of interest, let S denote the set of all CSs where sensors can be installed. The area is approximated by a grid on which targets can move. The grid graph $G = (V, A)$ is defined as follows. The vertex set V includes one vertex for each grid intersection point and two distinguished vertices o and t that represent the virtual origin and, respectively, destination of any path. The arc set A includes two arcs (i, j) and (j, i) for each grid edge $\{i, j\}$, the incoming/outgoing arcs connecting to the leftmost column vertices of the grid, and the rightmost column vertices to t, respectively. Note that CSs are not forced to lie on the grid. They can be positioned in any position of the area surrounding the grid, according to the available installation sites. Without loss of generality, we assume that G is a square grid of size $n \times n$. Given an illustration defined by (S, V, A) with two special vertices o and t and a budget value B, the first vital adaptation of the difficulty consists in deciding where to launch the sensors so as to exploit the exposure of the least-exposed path from two while guaranteeing a total installation cost of at most . To obtain a mathematical model for this difficulty version, we believe the decision variables: y_s, which is equal to 1 if a sensor is installed in candidate site s,and 0 or else; $x_{i,j}$,which is equal to 1 if arc belongs to the least-exposed path and 0 or else; and the nonnegative continuous variable z that expresses the exposure of the least-exposed path. These variables cause the following formulation: $\max_{s.t} \sum_{s \in S}^{z} c_s y_s \leq B$, $\min \sum_{(i,j) \in A} \left(\sum_{s \in S_{i,j}} e_{i,j}^{s} y_s \right) x_{i,j} \geq z$.

With the intention of avoiding cycling by believing feasible solutions that have previously been produced and try to run off from local maxima, a list of “tabu moves” is preserved. If the length of the list and the move approved out at a given iteration, the opposite of is forbidden (tabu) for the next iterations, until it is detached from the list. In accordance with the “aspiration criteria,” tabu moves can be obviously made if they cause a best found solution. The best solution encountered throughout the search procedure is accumulated and revisited subsequent to a maximum number of iterations max_{it}. The tabu list is applied in a simple way: Sensors that are deleted cannot be reinstalled through L iterations. To support search diversification, if the best solution found in the neighborhood does not improve the current solution throughout R moves, a random swap is carried out: A randomly chosen sensor is removed from y^{k}, while a sensor is installed in an empty CS chosen at random. We now consider the version of the intrusion detection problem with the objective of maximizing the detection probability of a mobile target that traverses the protected area, subject to a budget constraint on the total sensors’ installation cost. More precisely, we want to maximize the detection probability of any $o - t$ path with the lowest in the underlying grid G.

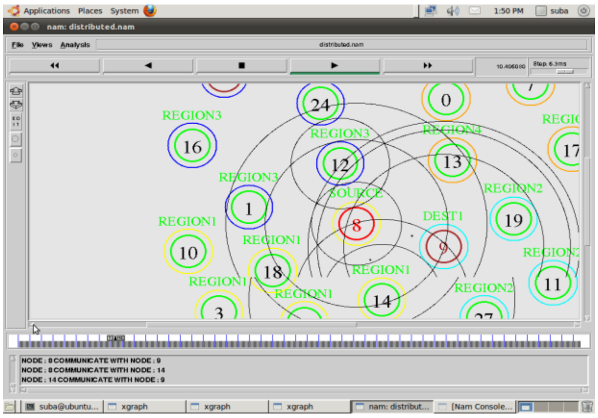

Fig 2: MILP formulation

Along with the possible heuristics able to resolve our optimization difficulty, we prefer in this paper the Tabu Search method [18, 19]. This method is a local search optimization method which tries to diminish a cost function $F(x)$, where x signifies a parameter vector, by iteratively moving from a elucidation x to a elucidation x in the neighborhood of x according to a neighborhood function $H(x)$ until a stopping criterion is satisfied or a predetermined number N of iterations is reached. The Tabu Search algorithm is independent of the event detection model. This model gives input parameters to the method, though some other detections models can be utilized. To deal with large-size instances of both formulations, we have developed Tabu Search (TS) algorithms. TS is a metaheuristic that guides a local search process to discover the solution space of optimization problems beyond local optima, which has been effectively adapted to a number of other challenging network design troubles. Starting from an initial feasible solution y^0, a set of neighboring solutions $N(y^0)$ is produced by concerning a set of possible “moves” to y^0. Then, the best solution in the “neighborhood” is selected as the next iteration y^1, even if it does not strictly improve the value of the objective function. The process is iterated to generate a sequence of solutions $\{y^k\}$.The rationale is to try to improve an initial solution by iteratively installing and removing sensors chosen on the basis of their revelation contribution to a least-exposed path of the current solution.

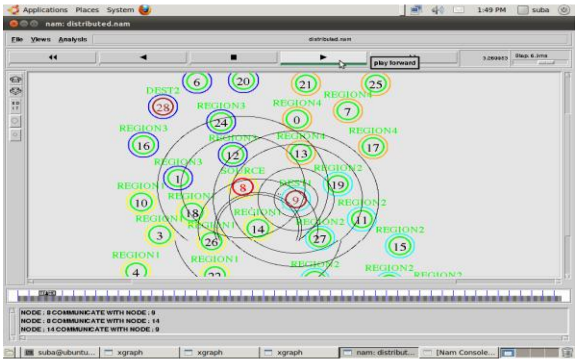

Fig 3: Heuristic Algorithm for Formulation

Game theory based intrusion detection schemes in WSN

The concentrate of the interaction among the intrusion detection negotiator and the attacker can be signified systematically by a game between two players. In these games, different strategies can be exercised by the intrusion detection agent with the aim of secure beside the different strategies that attackers always exploit. In the following, some game speculative based intrusion detection schemes in WSN are presented. The flexibility, fault tolerance, high sensing reliability, low-cost and rapid exploitation characteristics of WSNs are popular features in creating many new and exciting application areas for remote sensing, perceiving, tracking, and observing. But, it is non-trivial and very concerned to devise an optimal WSN to persuade performance ideas for example maximum sensing coverage and extended operating periods. With the intention of attaining a practical and feasible WSN and because of the operation nature of the network, game theory (GT) is considered as an attractive and a suitable basis to achieve the design goal. Game theory is a division of mathematics and can be exercised to examine system operations in dispersed and self-organizing networks. GT illustrates the behavior of players in a game. Players may be either cooperate or non-cooperative even as determined to exploit their results from the game.

In this view, sensors manage their processes in terms of power resources distributed to sensing and communicating between themselves and with a global regulator such that the dispatched assignment could be talented proficiently as favored [23]. Game theory is regularly attracting more attention as a method to resolve various problems in WSNs [23][24]. Typically, a game consists of a set of players, a set of strategies for each player and a set of equivalent utility functions. A model form game of a WSN of n sensor nodes is specified by a 3-tuple $G = < N, S, U >$. Here, G is a particular game, where $N = \{n_1, n_2, \ldots, n_n\}$ is a finite set of the sensor nodes. $S = \{S_1, S_2, \ldots, S_n\}$, is the strategy space of the sensor node i can select from is represented by S_i ($i = 1, 2, \ldots, n$). $U = \{u_1, u_2, \ldots, u_n\}$ is the subsequent payoff function of node i symbolized by u_i ($i = 1, 2, \ldots, n$), u_i is a utility value of each node obtains at the end of an action.

An approach for a player is an absolute plan of exploits in all possible circumstances in the game. The players attempt to act egoistically to make the most of their significances according to their preferences. We have to devise the payoff functions in a way that will help node i to select a strategy S_i that stands for the best reaction to the strategies selected by the other n-1 nodes. Here, s_i is the particular strategy selected by node i and $\mathbf{s}_{-i}$ is the particular strategies selected by all of the other nodes in the game. For strategies $\mathbf{s} = \{s_i, \mathbf{s}_{-i}\}$, it is described a strategy profile or on occasion a strategy combination. Each different combination of individual options of strategies can construct a different strategy profile. The strategy profile $\boldsymbol{s} = \{s_1, s_2, \ldots, s_n \mid s_i \in S_i, i = 1, 2, \ldots, n\}$ requires to position the nodes responding to a Nash Equilibrium (NE). It is a solution perception that explains a steady state condition of a game connecting two or more players, in which each player is unspecified to know the equilibrium strategies of the other players, and no player has whatever thing to achieve by changing only its own strategy independently. NE is distinguished wherein no nodes will sensibly prefer to turn aside from his selected strategy otherwise it will diminish its utility, *i.e.*, $u_i(s_i, \mathbf{s}_{-i}) \geq u_i(s_i^*, \mathbf{s}_{-i})$ for all $s_i^* \in S_i$.

A utility function describing player favorites for a given player allocates a number for every probable result of the game with the belongings that a higher number implies that the effect is more favored. In literature [25], the utility is described as:

$$u_i(s_i, s_{-i}) = \frac{br}{F_{s_i}} f(\gamma_j)$$

Where u_i (s_i, $\mathbf{s}_{-i}$) can be believed as the utility of node i transmitting information to a node j, b is the number of information bits in a packet of size F bits, r is the transmission rate in bits/sec using strategy s_i, and $f(\gamma_j)$ is efficiency function which enlarge with predictable SINR of the receiving node. The effectiveness purpose is identified as:

$$f(\gamma_j) = (1 - 2P_e)F$$

Where P_e is the bit error rate which depends on the channel state and interference from other nodes

Mechanism design not only gives the right incentives, but also to make certain the participants tell the truth. It can balance individual interests and common interests. The following terms related to the mechanism:

- **Definition 1 (Mechanism):** Mechanism can be expressed as $M = (\lambda, P)$, where M means some kind of mechanism, λ is the output function, $\lambda = \lambda\ (\lambda_1, \lambda_2, \ldots, \lambda_n)$, P is the payment function, $P = P\ (P_1 (\lambda), P_2 (\lambda), \ldots, P_n (\lambda))$.

- **Definition 2 (Strategy proof Mechanism):** In the mechanism M, any agent i, its true value t_i, the bid vector $\boldsymbol{b}_{-i}$, agent i in order to obtain maximum profit only by submitting a real bid (*i.e.*, $b_i = t_i$), the method is strategy proof.

- **Definition 3 (Voluntary participation condition):** In the mechanism M, any agent i, as long as it honestly bid, it cannot get negative profits, then this mechanism to meet the voluntary participation condition.

In a method, a member is identified an agent, there are usually n agents, each agent i (i = 1,2,…,n) has some private information which is recognized as the type of the agent or called the true value t_i, the private value is merely identified by agent, and is secret for the other agents. For instance, the type of an agent t_i can be the cost executing a consigned task. $v_i\,(t_i, \lambda)$ is the value function of an agent i, said the cost of executing a task. $p_i\,(\cdot)$ is the payment function for agent performing a task. $u_i\,(\cdot)$ is the utility function of an agent, that $u_i\,(\cdot) = p_i\,(\cdot) - v_i\,(t_i, \lambda)$. t_i is the true value, and $\tilde{t}_i$ is the execution value [55]. Define vector $t = (t_1, t_2, \ldots, t_n)$, $b = (b_1, b_2, \ldots, b_n)$, $\tilde{t} = \tilde{t}_1, \tilde{t}_2, \ldots, \tilde{t}_n)$, and the output vector $\lambda\ (\mathbf{b}) = (\lambda_1\ (\mathbf{b}), \lambda_2\ (\mathbf{b}), \ldots, \lambda_n\ (\mathbf{b}))$. Vector $\mathbf{b}_{-i}$ does not include the value b_i, which is $\mathbf{b} = (\mathbf{b}_{-i}, b_i)$. In a mechanism design, strategy proof situation will construct all participants' description their true value and voluntary involvement condition can make sure that all participants are eager to contribute.

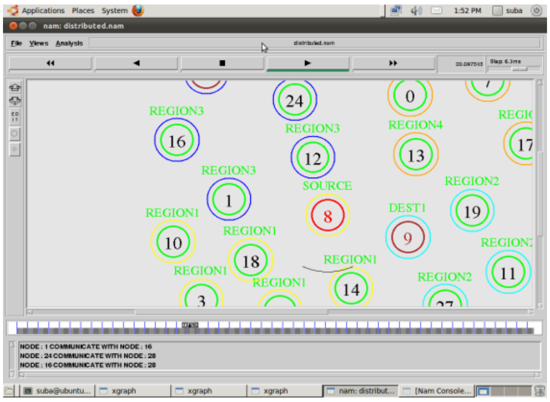

Fig 4: Intrusion Detection With HA With GT

The algorithm can comprise a weighted computation under the assumption that nearby nodes have greater effects than far away nodes, specifically giving the instantaneous neighbor the highest values in evaluating the intrusion detection states.

EXPERIMENTAL RESULTS AND DISCUSSION

The comparison is based on different metrics as the number of sensors deployed, packet delivery, and hop. For a regular exploitation we prefer a grid topology, so the shape is rectangular. We standardized the Tabu search process by fixing the number of iterations, the size of the Tabu list and the size of neighborhood investigated. For results of stochastic deployment strategies (Tabu Search and Random) we fixed a confidence level to 99:75%. Figure 5 shows the deployed sensor locations obtained by our Tabu Search approach. The number of nodes is represented in X axis and the delay in seconds represents in Y axis. The delay for the proposed is less when compared with the existing system.

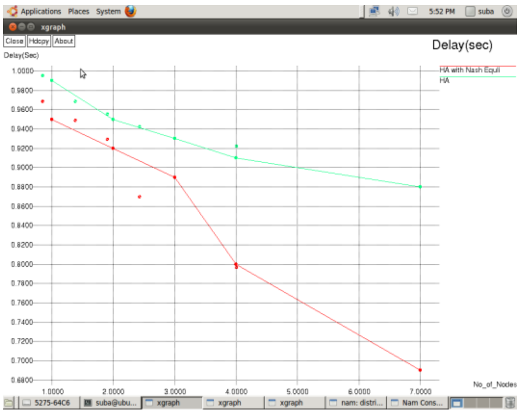

Fig 5: Delay comparison graph

Figure 6 shows the hop value of the sensor node with respect to the end to end distance. From the graph it can be said that as the network distance increases the energy consumed by the node also increases. It is so because when the node distance is improved the number of hop increases that is the transmitting and processing power increases relative. From the graph we can say that the HA with GT algorithm works better than the HA algorithm.

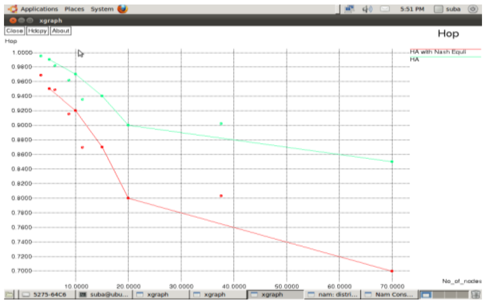

Fig 6: Hop based comparision

The packet delivery ratio is defined as the ratio of data packets received by the destinations to those produced from the sources. Mathematically, it can be defined as: PDR= $S1 \div S2$ Where, *S1 is* the sum of data packets accepted by the each destination and *S2 is* the sum of data packets produced by the each source. The Figure 7 shows the fraction of data packets that are successfully delivered during simulation time versus the number of nodes.

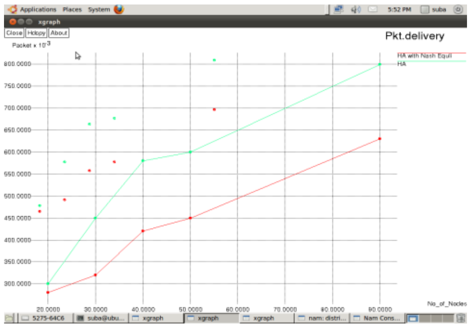

Fig 7: Packet Delivery Comparision

CONCLUSION

This paper has reviewed the recent developments in Game Theory for Wireless Sensor Networks. GT has the capability to observe a larger amount of probable scenarios before performing the action. Like a modeling tool, GT can make a decision procedure more sophisticated. The potential of applying GT to WSNs is forthcoming. In this paper, we concentrated on the intrusion detection problem in heterogeneous networks consisting of nodes with diverse security advantages. We devised the interaction between the attackers and the defenders as a noncooperative game and achieved an in-depth analysis on the NE and the engineering implications behind it. Founded on our game theoretical analysis, we derived expected behaviors of rational attackers. The experimental results show that the proposed work is 99.75% better than the existing method.

REFERENCES

1. B. Liu, P. Brass, O. Dousse, P. Nain, and D. Towsley, “Mobility Improves Coverage of Sensor Networks,” in Proc. ACM Int’l. Symp. Mob. Ad hoc Net. Comp. (ACM MobiHoc’05), pp. 300-308, 2005.

2. Dhillon, S. S., Chakrabarty, K., Iyengar, S. S. "Sensor Placement for Grid Coverage under Imprecise Detections." FUSION 2002.

3. Estrin, D., Govindan, R., Heidemann, J."Embedding the Internet." Communications of the ACM 2000.

4. Garey, M.R. and Johnson, D.S. "Computers and Intractability: A Guide to the Theory of NPCompleteness." W.H. Freeman and Company, 1979.

5. Gelfand, M. Fomin, S. "Calculus of Variations." Prentice-Hall Inc. 1963.

6. Li, X., Wan, P., Frieder, O. "Coverage Problems in Wireless Ad-Hoc Sensor Networks." IEEE Transactions for Computers 2002.

7. Megerian, S., Koushanfar, F., Qu, G., Potkonjak, M. "Exposure in Wireless Sensor Networks." MobiCom 2001.

8. Megerian, S., Koushanfar, F., Potkonjak, M.,Srivastava, M."Coverage Problems in Wireless AdHoc Sensor Networks."IEEE Infocom 2001

9. P. Balister, B. Bollobas, A. Sarkar, and S. Kumar,"Reliable Density Estimates for Achieving Coverage and Connectivity in Thin Strips of Finite Length. In Proc. of ACM Mobicom'07, Canada, September 2007.

10. J. L. Bredin, E. D. Demaine, M. Hajiaghayi, and D. Rus, "Deploying Sensor Networks with Guaranteed Capacity and Fault Tolerance", In Proc. of ACM MobiHoc'05, 2005.

11. Chen, S. Kumar, and T. H. Lai,"Designing Localized Algorithms for Barrier Coverage. In Proc. of ACM Mobicom'07, Canada, September 2007.

12. Y. Gao, K. Wu, and F. Li. "Analysis on the Redundancy of Wireless Sensor Networks. In Proc. of ACM WSNA'03, 2003.

13. R. Iyengar, K. Kar, and S. Banerjee,"Low-Coordination Topologies for Redundancy in Sensor Networks", In Proc. of MobiHoc'05, 2005.

14. S. Kumar, T. H. Lai, and A. Arora, "Barrier Coverage with Wireless Sensors", In Proc. of ACM MobiCom'05, 2005.

15. S. Kumar, T. H. Lai, M. E. Posner, and P. Sinha,"Optimal Sleep Wakeup Algorithms for Barriers of Wireless Sensors", In Proc. of BROADNETS'07, 2007.

16. N. Atay and B. Bayazit,"Mobile Wireless Sensor Network Connectivity Repair with K-Redundancy", Technical report, Washington University in St. Louis.

17. S. Meguerdichian, F. Koushanfar, G. Qu, and M. Potkonjak, "Exposure in wireless ad hoc sensor networks," in Proc. ACM MobiCom, 2001, pp. 139–150.

18. Y. C. Wang and Y. C. Tseng, "Distributed deployment schemes for mobile wireless sensor networks to ensure multilevel coverage," IEEE Trans. Parallel Distrib. Syst., vol. 19, no. 9, pp. 1280–1294, Sep. 2008.

19. F.G.Nakamura,F.P.Quintao,G.C.Menezes,and G.R.Mateus,"An optimal node scheduling for flat wireless sensor networks," Lecture Notes Comput. Sci., vol. 3420, pp. 475–482, 2005.

20. Apt K., Witzel A. "A generic approach to coalition formation", Proceedings of the International Workshop Computational Social Choice (COMSOC); Amsterdam, The Netherlands. 6–8 December 2006.

21. Gu D. "A game theory approach to target tracking in sensor networks". IEEE Trans. Syst. Man Cyber. B Cybern. 2011;41:2–13

22. Kazemeyni F., Johnsen E., Owe O., Balasingham I. "Group Selection by Nodes in Wireless Sensor Networks Using Coalitional Game Theory". Proceedings of 2011 16th IEEE International Conference on Engineering of Complex Computer Systems (ICECCS 2011); Las Vegas, NV, USA. 27–29 April 2011.

23. Kannan R., Sarangi S., Iyengar S.S. "Sensor-centric energy-constrained reliable query routing for wireless sensor networks". J. Paral. Distrib. Comput. 2004;64:839–852

24. Wang W., Li X. "Low-cost routing in selfish and rational wireless *ad hoc* networks", IEEE Trans. Mobile Comput. 2006;5:596–607

25. Sengupta S., Chatterjee M., Kwiat K. "A game theoretic framework for power control in wireless sensor networks". IEEE Trans. Comput. 2010;59:231–242

26. McCune J.M., Shi E., Perrig A., "Reiter M. Detection of denial-of-message attacks on sensor network broadcasts". Proceedings of 2005 IEEE Symposium on Security and Privacy; Oakland, CA, USA. 8–11 May 2005.

27. Kodialam M., Lakshman T.V. "Detecting network intrusions via sampling: A game theoretic approach". Proceedings of Annual Joint Conference of the IEEE Computer and Communications (INFOCOM 2003); 30 March–3 April 2003.
28. Maskery M., Krishnamurthy V. "Decentralized adaptation in sensor networks: Analysis and application of regret-based algorithms". Proceedings of 2007 46th IEEE Conference on Decision and Control; New Orleans, LA, USA. 12–14 December 2007.
29. Czarlinska A., Luh W., Kundur D. "Attacks on sensing in hostile wireless sensor-actuator environments". Proceedings of Globecom 2007: 2007 IEEE Global Telecommunications Conference; Washington, DC, USA. 26–30 November 2007.
30. Ren H., Meng M., Chen X. "Cross-layer optimization schemes for wireless biosensor networks". Proceedings of 6th World Congress on Intelligent Control and Automation; Dalian, China. 21–23 June 2006.
31. Li X., Lyu M.R. "A novel coalitional game model for security issues in wireless networks". Proceedings of 2008 IEEE Global Telecommunications Conference; New Orleans, LA, USA. 30 November–4 December 2008.
32. Wang W., Chatterjee M., Kwiat K. "Coexistence with Malicious Nodes: A Game Theoretic Approach". Proceedings of International Conference on Game Theory for Networks (GameNets '09); Istanbul, Turkey. 13–15 May 2009; pp. 277–286.

J.NAVEEN Received his B.E Computer Science & Engineering From Anna University, Chennai in 2008 and Pursuing M.E Computer Science & Engineering From Anna University, Chennai, India His PG Project interest are In the area of Wireless sensor network's