EXPLORATIONS ON ENGINEERING LETTERS (EEL)
VOLUME 1, ISSUE 1 (2016):PP.99-105
SANA ACADEMIC PRESS

Optimization and Enhancing Security in Wireless Sensor Network Using Game Theory

K. Anitha Devi[1], A. Sivasankari[2], R. Latha[3]
[1]Research Scholar, St. Peter's University, Chennai.7
[2]Asst.Prof, Dept. of Computer Application, St. Peter's University, Chennai
[3]Prof. & Head., Dept. of Computer Science & Applications, St. Peter's University, Chennai
samoshik@gmail.com

Abstract-- *A wireless sensor network (WSNs) is popular developing field in industrial and other major markets. Wireless data security is the main theme in the WSNs application where security of transmitted data is more concerned. Due to the major concentration over 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 (GT) is a mathematical method that describes the phenomenon of conflict and cooperation between intelligent rational decision-makers. In particular, the theory has been proven very useful in the design of wireless sensor networks (WSNs). The roles of GT are described that include routing protocol design, topology control, power control and energy saving, packet forwarding, data collection, spectrum allocation, bandwidth allocation, quality of service control, coverage optimization, WSN security, and other sensor management tasks. Then, three variations of game theory are described, namely, the cooperative, Non-cooperative, and repeated schemes. Finally, existing problems and future trends are identified for researchers and engineers in the field. Game theory is applied here to select different routes to transfer the data from source to destination. The performance of the WSNs was increased on the basis of security and transmitted data. The graph for throughput, end to end delay, delivery and packet loss ratio are generated using NS2 simulation.*

Keywords: *WSN, Game Theory, NS2 Simulation, Power Control, Energy Saving.*

I. INTRODUCTION

Wireless sensor network theory has attracted much attention in different areas of science and engineering as an emerging research area. Applications of sensor networks include home energy management, monitoring environmental phenomena and traffic control, to name only a few. Utilization of sensor networks in data gathering applications deals with several aspects of network performance like capacity and lifetime efficiency. Performance optimization is basically performed by adopting a proper resource management strategy for the sensors as stand-alone battery-powered devices. Specifically, lifetime optimization is typically carried out by formulating the energy consumption of a sensor (as a function of its sensing and communication power) and defining the network lifetime accordingly. A commonly-used definition for the network lifetime is the time it takes for the first sensor to run out of battery. Maximizing the capacity and the network lifetime are two conflicting goals. Increasing the network capacity requires increasing the data transmission rates at the nodes which increase the energy consumption and hence, reduces the network lifetime. Lifetime-improving routing strategies in wireless networks usually set a fixed throughput level at the transmitting nodes and optimize the network lifetime by efficient routing. The trade-off between the network lifetime and its capacity is well-studied in.

In data gathering applications, the sensors are required to continuously measure environmental variables and transmit them to a base station (sink node) in a cooperative fashion. This requires a proper routing scheme to establish a route from any node in the network to the sink node. The information transmitted by each node includes its own data stream as well as the intended traffic received from other nodes in the network. The overall performance measure of a network (e.g., energy consumption and network lifetime) highly depends on the routing strategy. Lifetime-optimizing routing strategies are basically network layer protocols which aim at balancing the traffic load in wireless networks by finding efficient paths from source (or relay) nodes to sink nodes. To achieve better lifetime performance, several classes of strategies have been introduced, which involve combining route selection and resource allocation schemes. Such classes utilize mobility, topology control or cross-layer design as additional means in addition to route selection strategies. In the sequel, present a brief overview of the main categories of methods.

Related Studies: Game theory and intrusion detection systems

Mobile ad hoc networks (MANETs) are a collection of mobile nodes that communicates over wireless media. Performance of MANET depends on the cooperative participation of nodes in packet forwarding. During packet forwarding from source to destination, it takes help of middle hop depending on the distance. Middle hops play different role in different times. Nodes in MANETs suffer from limited resources specially battery power. To save its resources, middle hop acts like selfish node in which nodes are simply dropping packets instead of forwarding the same to its neighbour. Malicious nodes drop packets maliciously instead of forwarding them to destination. Performance parameters of network are effected by malicious behaviour of nodes. Intrusion detection system (IDS) are designed to detect malicious nodes. Some of these IDS suffer from some arbitrariness. Game theoretic approach helps to remove this arbitrariness from the IDS and to define the equilibrium state of the network. Objective of this paper is to discuss the game theory in MANETs and also to discuss about game theoretic approach to detect malicious nodes in MANETs.

An Intrusion Detection Game with Limited Observations

They present a 2-player zero-sum stochastic (Markov) security game which models the interaction between malicious attackers to a system and the IDS who allocates system resources for detection and response. Capture the operation of a sensor network observing and reporting the attack information to the IDS as a finite Markov chain. Thus, extend the game theoretic framework in [*Akyildiz I*] to a stochastic and dynamic one. The outcomes and evolution of an example game numerically for various game parameters. Furthermore, the study limited information cases where players optimize their strategies offline or online depending on the type of information available, using methods based on Markov decision process and Q-learning.

Intrusion Response as a Resource Allocation Problem

The study intrusion response in access control systems as a resource allocation problem, and address it within a decision and control framework. By modelling the interaction between malicious attacker(s)

and the intrusion detection system (IDS) as a non cooperative non-zero sum game, develop an algorithm for optimal allocation of the system administrator's time available for responding to attacks, which is treated as a scarce resource. This algorithm, referred to as the Automatic or Administrator Response (AOAR) algorithm, applies neural network and LP optimization tools. Finally, implement an IDS prototype in MATLAB based on a game theoretical framework, and demonstrate its operation under various scenarios with and without the AOAR algorithm. Our approach and the theory developed are general and can be applied to a variety of IDSs and computer networks.

A Logical Framework for Evaluating Network Resilience Against Faults and Attacks

They present a logic-based framework to evaluate the resilience of computer networks in the face of incidents, i.e., attacks from malicious intruders as well as random faults. Our model uses a two-layered presentation of dependencies between files and services, and of timed games to represent not just incidents, but also the dynamic responses from administrators and their respective delays. Demonstrate that a variant TATL♦ of timed alternating-time temporal logic is a convenient language to express several desirable properties of networks, including several forms of survivability. illustrate this on a simple redundant Web service architecture, and show that checking such timed games against the so-called TATL♦ variant of the timed alternating time temporal logic TATL is EXPTIME-complete.

Internet infrastructure security: a taxonomy

The pervasive and ubiquitous nature of the Internet coupled with growing concerns about cyber terrorism demand immediate solutions for securing the Internet infrastructure. So far, the research in Internet security primarily focused on. securing the information rather than securing the infrastructure itself. Given the prevailing threat situation, there is a compelling need to develop architectures, algorithms, and protocols to realize a dependable Internet infrastructure. In order to achieve this goal, the first and foremost step is to develop a comprehensive understanding of the security threats and existing solutions. This article attempts to fulfil this important step by providing a taxonomy of security attacks, which are classified into four main categories: DNS hacking, routing table poisoning, packet mistreatment, and denial-of-service attacks. The article discusses the existing solutions for each of these categories, and also outlines a methodology for developing secure protocols.

Existing system

Considering a collection of neighbouring data segments as random variables, determine those behaving abnormally by exploiting their spatial predictabilities and, motivated by spatial analysis, specifically investigate how to implement a prediction variance detector in a WSN. As the communication, cost incurred in aggregating a covariance matrix is finally optimised using the Spearman's rank correlation coefficient and differential compression.

Disadvantages of Existing Method

The classical techniques used to identify the anomalies in the network is time consuming work. This system only identifies the anomalies but does not avoid the loss of data in network. So anomalies identification before the data loss is not possible. Need more processing skills. In existing research network life time and security cannot be obtained simultaneously.

Proposed system

In our research, game theory has been used. Game theory has been used for achieving the trade-off between maximizing the network life time and providing security. In previous times, network life time and security cannot be obtained simultaneously. But with the help of game theory, both can be obtained simultaneously. Hacking can be prevented in our research by using game theory. Even if hacking has been done, it is unable for the person who is hacking to obtain the data since the destination will not receive any data if any router is off.

Advantages of Proposed Method

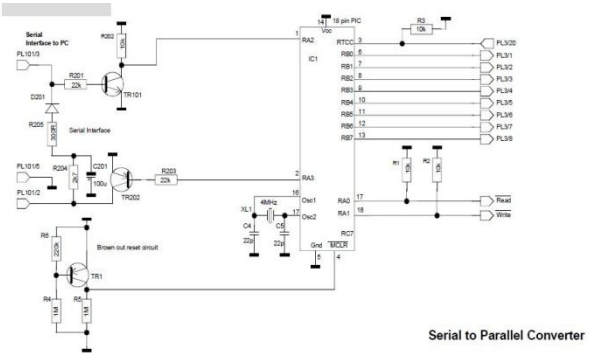
A common protocol which overcomes energy deficiency and anomaly problems in the network. Light weight process which easily handles the data by split and merge method.

Methodology

In this research, game theory has been used for implementation. Since sensor nodes have limited resources, cooperation may come at a significant expense; but, it gives also an intention to some nodes to act selfishly. In the area of Wireless Sensor Networks (WSNs), improving energy efficiency and network lifetime is one of the most important and challenging issues. Game theory can be used in WSNs to achieve a trade-off between maximizing the network lifetime and providing the required service. In our research, source, destination and two routers have been used. Source sends a data to the destination with the help of two routers. Source splits the data in two parts and forwards one part to one router and another part to another router. The routers forward the parts to the destination and destination combines both the parts and obtains the data. If anyone of the router is off, the destination will not receive any one part of data. So it will not show anything in the output.

In this research, game theory has been used for implementation. Since sensor nodes have limited resources, cooperation may come at a significant expense; but, it gives also an intention to some nodes to act selfishly. In the area of Wireless Sensor Networks (WSNs), improving energy efficiency and network lifetime is one of the most important and challenging issues. Source sends a data to the destination with the help of two routers. Source splits the data in two parts and forwards one part to one router and another part to another router. The routers forward the parts to the destination and destination combines both the parts and obtains the data. If anyone of the router is off, the destination will not receive any one part of data. So it will not show anything in the output. The goal of the system requirements specification is to completely specify the technical requirements for the software product in a concise and unambiguous manner. Picc complier the example research the development and simulation of a complete program using FED PIC C. Purchasers of WIZ C are recommended to run through the tutorial of that program before running this example for which the Application Designer should be disabled (once the research has been opened use the Research | Use Application Designer menu option to turn it off).The program is designed for a 16F84 processor (although in practice any 18 pin PIC could be used with the same program), and is intended as a simple serial to parallel converter utility.

The research is designed to communicate with another computer system such as a PC or a Mac, using a3-wire serial interface. Simple commands will be accepted on the serial link. 8 of the I/O ports on the16F877a will be configured as inputs or outputs. The program operates on a processor running at 4MHz and the serial link runs at 9600bps.
The circuit of the application is shown below:



Although to simulate this circuit it may also be tested by building on the demonstration board shown in the tutorial section. Note that if a PIC which does not have PORTB pull ups is used then Port B pins must be pulled up with an external resistor array (Nearly all PIC's have this capability). Port A bit 2 is the received data bit, Port A bit 3 is the transmitted data bit. The commands that will be accepted on the link will be:
A-This character forces the PIC to send a K character back on the serial link to confirm that the PIC is present. W This character is followed by another byte, the second byte is written to Port B as an output, whilst bit 1 of Port A is set low and then high again as a clock signal. R This forces the PIC to read Port B, whilst it strobes Port A, bit 0 low. In either event a K character is sent back on the serial interface. If any other character is received then an F character is sent back on the link.

Start the program and open a new research

Start FED PIC C by double clicking the icon.To open the new research then use the Research | Open/New Research menu item (on the professional version this will be Open/New Research Group). A File dialog box will be brought up. Create a new directory by using the small icon of a folder with a star in the right hand corner. Call the directory "SerialToParallel" or whatever name is meaningful. Select the new directory, double click to enter it,and then select the research file name "StoP". Press OK. If you are a WIZ-C user then now is the time to use the Research | Use Application Designer menu option to turn off the front end. Press ALT and E to set the windows up in editing view (try pressing ALT+C and ALT+D as well –these are different ways of laying out the windows). Initially this research consists of one C file. Use File | New to create a blank file, now use File | Save As to select a file name. This will bring up a file open dialog box. No files will be present so enter the filename "SToP" and click on OK.
Select the research window which has the title StoP and will be blank and press the insert key. This will bring up a file open dialog box. One file "STop.C" will be present so select this file and click on OK.

A dialog box will now appear with this file name and a number of options, files as being C files, or as a comment file. In this case the file is used for compilation, so make sure that the file type C is selected and click OK. Double click the file to open it, now enter the following code to start after finish code includes the header file for the PIC16F84, and the header file which includes the definitions for the serial interface routines. It also initialises Port A to be all outputs except for bit 2 which is an input used for serial receive data.

Compile and complete the research

Now use the menu option Compile | Compile (or press Ctrl+F9) to compile the research. An options dialog box will appear. Ignore all the options in the box except for the processor type, select the type PIC16F84 and press OK. This box will not be shown again unless the menu option Research | Set Options for Research is used. The information window should show the progress of the compilation, all being well the research will compile OK. Now finish the research by entering the following code (alternatively clear the edit window by selecting all the text and press delete, and then use File | Insert to enter the file "STop.C" which is in the home directory for FED PIC C). Note that this program contains an error. Save it using the file menu, save option. Compile it again and this time the error will be shown in the error window. Double click the error and the edit window will be moved to show the line with the error - SerialOut(tx) should read pSerialOut. Put the cursor on the word SerialOut and press Control and F1, the help file will be bought up at the right entry for both functions. The help file explains the need for the constants defined at the top of the file to tell the serial routines which port and bits to be used. Correct the error and compile again, this time the program will compile successfully and will be assembled into a hex file ready for debugging.

Game theory

Algorithmic game theory is an area in the intersection of game theory and algorithm design, whose objective is to design algorithms in strategic environments. Typically, in Algorithmic Game Theory problems, the input to a given algorithm is distributed among many players who have a personal interest in the output. In those situations, the agents might not report the input truthfully because of their own personal interests. On top of the usual requirements in classical algorithm design, say *polynomial-time running time, good approximation ratio*, ... the designer must also care about incentive constraints. The Algorithmic Game Theory from two perspectives:

Analysis: look at the current implemented algorithms and analyze them using Game Theory tools: calculate and prove properties on their Nash equilibria, price of anarchy, best-response dynamics ...

Design: design games that have both good game-theoretical and algorithmic properties. This area is called algorithmic mechanism designs The field was started when Nisan and Ronen in STOC'99 drew the attention of the Theoretical Computer Science community to designing algorithms for selfish (strategic) users. As they claim in the abstract:

Following notions from the field of mechanism design, it is suggested a framework for studying such algorithms. In this model the algorithmic solution is adorned with payments to the participants and is termed a mechanism. The payments should be carefully chosen as to motivate all participants to act as

the algorithm designer wishes. The standard tools of mechanism design to algorithmic problems and in particular to the shortest path problem.

CONCLUSION

In this paper, the intrusion detection problem in heterogeneous networks consisting of nodes with different security assets is described. The interaction between the attackers and the defenders as a non-cooperative game and performed an in-depth analysis on the NE and the engineering implications behind it. Based on the game theoretical analysis, the expected behaviours of rational attackers is derived. Sufficient monitor resource and appropriate configuration at the defender side are two necessary conditions of efficiently protecting the network. The minimum monitor resource requirement and the optimal strategy of the defender side to achieve system optimality. It also provided a case study to show how to apply the proposed game theoretical framework to configure the intrusion detection strategies in realistic scenarios. A natural and interesting research direction is to use the results in this paper as foundations to investigate the dynamic and limited information intrusion detection game.

REFERENCES

[1] Akyildiz I et al, 2002, “Wireless sensor networks: a survey,” Computer Networks, vol. 38, no. 4, pp. 393– 422.

[2] Chang J et al., 2004, “Maximum lifetime routing in wireless sensor networks,” IEEE/ACM Transactions on Networking, vol. 12, no. 4, pp. 609–619.

[3] Gungor V et al., 2009 “Industrial wireless sensor networks: Challenges, design principles, and technical approaches,” IEEE Transactions on Industrial Electronics, vol. 56, no. 10, pp. 4258–4265.

[4] Gupta P et al., 2000, “The capacity of wireless networks,” IEEE Transactions on Information Theory, vol. 46, no. 2, pp. 388–404.

[5] Hancke G et al., 2010 “Opportunities and challenges of wireless sensor networks in smart grid,” IEEE Transactions on Industrial Electronics, vol. 57, no. 10, pp. 3557–3564.

[6] Polastre J et al., 2004, “Analysis of wireless sensor networks for habitat monitoring,” Wireless Sensor Networks, pp. 399–423, 2004.

[7] Schurgers C et al., 2002, V. Tsiatsis, “Optimizing sensor networks in the energy-latency-density design space,” IEEE Transactions on Mobile Computing, vol. 1, no. 1, pp. 70–80.

[8] Tubaishat M et al.,2009, “Wireless sensor networks in intelligent transportation systems,” Wireless Communications and Mobile Computing, vol. 9, no. 3, pp. 287–302.