International Journal of Enhanced Research in Management & Computer Applications
ISSN: 2319-7471, Vol. 6 Issue 3, March-2017, Impact Factor: 1.544

Performance Analysis of Game theoretic modelling and algorithmic comparison in Wireless Sensor Networks

Asha Rani

Dept. of Computer Engineering, R N College of Engineering, Rohtak, Haryana

ABSTRACT

In this paper, game theory for solving the network security problem of wireless sensor networks has been studied. The author explored game theory algorithms to model situation for wireless network with malicious nodes and investigate the attack and detection problem by modeling it as pairwise simultaneous game and spatial structured game and considered the relationship between the nodes in a wireless sensor network to formulate the game and give the game theory algorithms in detail. Author also evaluate the approach with a simulation experiment and analyze the simulation results in detail. This approach is able to support secure end-to-end communication in wireless sensor networks.

Keywords: E-commerce, WSN, jamming, attack, game theoretic modeling.

1. INTRODUCTION

The unattended nature of wireless sensor networks (WSNs) makes them very vulnerable to an adversary's malicious attacks. An adversary can physically compromise a subset of nodes in a WSN to eavesdrop information. The compromised nodes (or malicious nodes) become black holes in the network. Those black holes in a WSN raise hidden-action attacks to reduce the performance of the network or even destroy the network. Therefore, network security is an important issue for WSNs. In a WSN with malicious nodes, there are obvious conflicts between malicious nodes and normal nodes. As a branch of applied mathematics, game theory is concerned with how rational entities make decisions in a situation of conflict, which has been used primarily in economics. Game theory aims to model situations in which decision makers have to make specific actions that have mutual—possibly conflicting—consequences. In the con- text of WSNs, game theory may be used to form cooperation schemes among entities in a competitive environment, for example, power control, routing, and resource allocation. Game theory can be applied to model the situation where there are malicious nodes in a WSN.

Jamming in wireless networks is defined as the disruption of existing wireless communications by decreasing the signal-to-noise ratio at receiver sides through the transmission of interfering wireless signals. Jamming is different from regular network interferences because it describes the deliberate use of wireless signals in an attempt to disrupt communications whereas interference refer to unintentional forms of disruptions. Unintentional interference may be caused by the wireless communications among nodes within the same networks or other devices (e.g. microwave and remote controller). On the other hand, intentional interference is usually conducted by an attacker who intends to interrupt or prevent communications in networks. Jamming can be done at different levels, from hindering transmission to distorting packets in legitimate communications.

The effluence of the jamming detection mainly depends on the causes of the network parameters that is quick deactivation of the jammer that can be taken. This place the limitation in the application of jamming detection where there is no middle action is necessary.[11] The main common measure to the jamming is to extenuate the impact of jammer by using antijamming communication technique contain highly directed antenna spread-frequency spectrum, and error-correcting codes. Periodicity hopping spectrum and direct successions widen spectrum are the common anti-jamming communiqué techniques that enable the sender of the message to increase signal in time such that it is transmitted in the unpredictable to the jammer. Basically attacker cannot physically segregate a device, attacker alter or delete the message and it is restricted by the interference with the message transformation and hence the performance can be reduced.

The Wireless networks give the concept of distributed architecture so that the sharing of information as well as resources can be done effectively. With the advancement of internet and the growth of personal computers, the use of sensor computers is been increased very fast. A sensor network [is defined as a wide public area network in which number of sensor nodes is connected. Mobility is the key property of such kind of network. These kinds of networks perform the communication with multiple nodes under multiple controller devices.

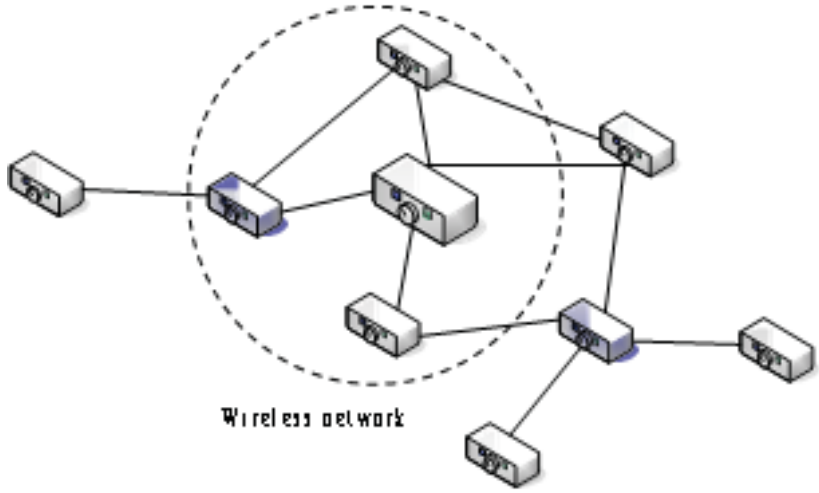

Fig. 1: A wireless sensor network with malicious nodes.

The connection will be performed over the multiple nodes. There are different kind of network exist based on the application areas as well as network scenarios and the configuration. These network types are listed in figure 1.

The elementary attribute of wireless sensor network that render them defenseless to attack is the major nature of shared medium. This broadcast the network to passive and active attack, these are different in nature and objectives. Generally the malicious node or entity does not take any action but attack node continuously observe communication which is ongoing state as eavesdropping so as to mediate with the preservation of privacy of the network that involved in the communication .

The main communicating criteria of WSN are the selection of next node. This can be done in static or dynamic way. The static routing can be performed by maintaining a routing table and the dynamic routing is identified as the on demand routing. This kind of routing start with the source node and with the definition of coverage range the next neighbor node will be selected for the communication. This process is repeated till the Destination node not arrived.

A sensor network is one of the critical adhoc network in which nodes communicated cooperatively to deliver the information. But because of this cooperative nature, the network suffers from various kind of attacks. One of such critical attack is jamming attack. The presented work is defined to provide game theoretical model based approach to provide safe communication under jamming attack. In this work, a constraint specific behavior analysis approach is defined. The work is here defined in two main stages. In first stage, the network will be divided in smaller segments and constraint specific behaviour analysis will be performed. Once the critical segments will be identified, the game theory based constraint specific modelling will be defined to identify the jamming attack.

A jamming attack is particularly effective from the attacker's point of view since, the adversary does not need special hardware to launch it, the attack can be implemented by simply listening to the open medium and broadcasting in the same frequency band as the network uses, and If launched wisely, it can lead to significant benefits with small incurred cost for the attacker. With regard to the machinery and impact of jamming attacks, they usually aim at the physical layer in the sense that they are realized by means of a high transmission power signal that corrupts a communication link or an entire area. Conventional defense techniques against physical layer jamming rely on spread spectrum which can be too energy consuming for resource-constrained sensors.

Jamming attacks also occur at the access layer, whereby an adversary either corrupts control packets or reserves the channel for the maximum allowable number of slots, so that other nodes experience lower throughput by not being able to access the channel. The work in [11] studies the problem of a legitimate node and a jammer transmitting to a common receiver in an on-off mode in a game-theoretic framework. Other jamming instances can have impact on the network layer by malicious packet injection along certain routes or at the transport layer by SYN message flooding for instance.

GAME THEORETIC MODELLING ANALYSIS

In this section, we investigate the attack and detection problem by modeling it as a simultaneous game. In this game, we consider the relationship between every pair of nodes in the network. We try to formulate different cases for this game in detail.

Pairwise Simultaneous Game: Let us consider a WSN with two nodes, a normal node n and a malicious node m. It is a pairwise simultaneous game between the two nodes, where both players move simultaneously. Each player has four strategies (see Table 1). Here γ is the direct income for a node to send out a data packet successfully; that is, the packet is received by another node. αF is the probability that a normal node sends out a data packet successfully ($1 > \alpha F > 0$). αJ is the probability that a malicious node sends out a jamming packet successfully ($1 > \alpha J > \alpha F$). It makes sense that jamming is more likely to be successful than forwarding.

Here p is a punishment to a detected jamming action of the malicious node, and s is a stimulus to a successful jamming detection of the normal node ($p > 0$, $s > 0$).

We formulate the energy consumption in the game by some constants. $\beta 1$ is the cost to receive a packet (receiving

or detecting, $\beta 1 > 0$), and $\Delta\beta 1$ is the additional cost for detecting attacks ($\Delta\beta 1 > 0$). $\beta 2$ is the cost to send out a packet (forwarding or jamming, $\beta 2 > 0$), and $\Delta\beta 2$ is the additional cost for jamming because jamming action consumes more

energy compared with normal forwarding action ($\Delta\beta 2 > 0$).

Game Theory Algorithms

We could formulate the game for a WSN given in Section 3 by the following algorithms. First, let us consider the case for one specific wireless node (either normal node or malicious node). Algorithm 1 is proposed to compute the payoff of a specific wireless node.

The algorithm is trivial. The payoff of a specific node is impacted by the roles of its neighbors. In order to compute the payoff of a specific node, we have to consider the relationship between the node and each of its neighbors.

Then we could compute the payoffs of the whole network based on Algorithm 1. The algorithm for computing global payoffs is given as follows.

Input: A wireless node $n0$.

Output: A payoff value $p0$.

get the neighbour nodes of $n0$ as $NB = \{n1, n2,..., nk\}$

for each node ni in NB ($i = 0, 1,..., k$)

perform a two nodes' game between $n0$ and ni

end loop

construct a many-to-many game for $n0$ and NB

compute payoff $p0$ for $n0$ under the restriction of the rules

return$p0$

Algorithm 2 is also easy to be understood. The process of computing global payoffs is reduced to traversing an undirected graph by BFS.

Input: A WSN with a collection of nodes $N= \{n0, n1,..., nk\}$, a source node $n0$, and a collection of malicious nodes $M= \{mi, mi+1,..., mh\}$, where $n0 \in N$, $M \subset N$.

Output: A collection of payoff values $P = \{p0, p1,..., pk\}$ for N, where pi is the payoff of

ni (i = 0, 1,..., k).

Assign an initial action to each ni in N and the action of $n0$ is *Forward*

Set $n0$ as the root node

Perform BFS by starting with $n0$

for each intermediate node ni in BFS

compute payoff for ni by using **Algorithm 1 get** pi for ni

end loop

Return $P = \{p0, p1,..., pk\}$

For each node, we just perform a single-node payoff computation, and then we get the information for the whole network. To a given WSN, we shall perform a series of computations to reach convergence.

CONCLUSION

In this paper, an effective approach to apply game theory into solving the network security problem of WSN. The author tries to explore and compare game theory algorithms to model the situation for WSN with malicious nodes, in order to support reliable and secure wireless communications against the attacks of malicious nodes in the network.

REFERENCES

[1]. Yean-Fu Wen, "Energy-Efficient Data Aggregation Routing and Duty-Cycle Scheduling in Cluster-based Sensor Networks", IEEE Conference on Consumer Communication and Networking, pp 95-99, 2007.
[2]. Chunsheng Zhu, "Sleep Scheduling Towards Geographic Routing in Duty-Cycled Sensor Networks", International Conference on Distributed Computing and Workshops, pp 1-3, 2011.
[3]. Chunsheng Zhu, "Sleep Scheduling Towards Geographic Routing in Duty-Cycled Sensor Networks With A Mobile Sink", IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks, pp 1-6, 2011.
[4]. Yuanyuan Zeng, "Joint Power Control, Scheduling and Real-time Routing in Wireless Sensor Networks", International Conference on Advance Computer Control, pp 357-361, 2010.
[5]. Feng Liu, "Joint Routing and Sleep Scheduling for Lifetime Maximization of Wireless Sensor Networks", IEEE Transactions on Wireless Communications, pp 2258-2267, 2010.
[6]. Yu Gu, "Joint Scheduling and Routing for Lifetime Elongation in Surveillance Sensor Networks", IEEE Asia-Pacific Services Computing Conference, pp 81-88, 2007.
[7]. Saeyoung Ahn, "Slotted Beacon Scheduling Using ZigBee Cskip Mechanism", The Second International Conference on Sensor Technologies and , pp 103-108, 2008.
[8]. Yavuz Bogaç Turkogullari, "An Efficient Heuristic for Placement, Scheduling and Routing in Wireless Sensor Networks", International Symposium on Computer and Information Science, pp 1-6, 2008.
[9]. Yawen Dai, "MEBRS: Energy Balancing Route Scheduling in Centralized Wireless Sensor Networks", 1st Int'l Symposium on Quality Electronic Design-Asia, pp 270-275, 2009.
[10]. J. M. McCune, E. Shi, A. Perrig and M. K. Reiter, "Detection of denialof-message attacks on sensor network broadcasts," Proc. IEEE Symposium on Security and Privacy, 2005.
[11]. A. Wald, Sequential Analysis, Wiley 1947, Vladimir P. Dragalin, A. G. Tartakovsky and V. V. Veeravalli. "Multihypothesis Sequential Probability Ratio Tests - Part I: Asymptotic optimality," IEEE Trans. Inf. Theory, Vol. 45, No. 7, Nov. 1999.
[12]. C. W. Helstrom, Elements of signal detection and estimation, pp. 339-340, Prentice-Hall, 1995.
[13]. A. M. Mathai, An introduction to geometrical probability, Gordan and Breach Science Publishers, 1999.
[14]. B. Awerbuch, A. Richa, and C. Scheideler, "A Jamming-Resistant MAC Protocol for Single-Hop Wireless Networks," in Proc. Of Principles of Distributed Computing, 2008.
[15]. Bayraktaroglu, C. King, X. Liu, G. Noubir, R. Rajaraman, and B.Thapa, "On the Performance of IEEE 802.11 under Jamming," in Proc. of IEEE INFOCOM, 2008.
[16]. S. Radosavac, I. Koutsopoulos, and J.S. Baras, "A Framework for MAC Protocol Misbehavior Detection in Wireless Networks," Proc ACM Workshop Wireless Security (WiSe), 2005.
[17]. A.D. Wood and J.A. Stankovic, "Denial of Service in Sensor Networks," Computer, vol. 35, no. 10, pp. 54-62, Oct 2002.
[18]. R. Negi and A. Perrig, "Jamming Analysis of MAC Protocols," Carnegie Mellon Technical Memo, 2003.
[19]. R. Mallik, R. Scholtz, and G. Papavassilopoulos, "Analysis of an On Off Jamming Situation as a Dynamic Game," IEEE Trans. Comm., vol. 48, no. 8, pp. 1360-1373, Aug. 2000.
[20]. Jung, V. Paxson, A.W. Berger, and H. Balakrishnan, "Fast Portscan Detection Using Sequential Hypothesis Testing," Proc. IEEE Symp Security and Privacy, 2004.