International Journal of Contemporary Research in Computer Science and Technology (IJCRCST) e-ISSN: 2395-5325
Volume1, Issue 6 (September '2015)

A REVIEW ON INTRUSION DETECTION SYSTEMS IN WIRELESS SENSOR NETWORKS USING GAME THEORY APPROACH

Ms. J. Saranya,
M.Phil. Research Scholar & Assistant Professor,
Department of Computer Science,
Sri Krishna Arts & Science College, Coimbatore, India.

Mrs. J. Lekha,
Asst. Professor, Dept. of Computer Science Application & Software System,
Sri Krishna Arts & Science College, Coimbatore, India.

Abstract: Wireless Sensor Networks (WSNs) consist of sensor nodes deployed in a manner to collect information about surrounding environment. Wireless Sensor Networks is used in wide range of applications because of the various features like low cost, no gateways or switches for monitoring the flow of information when the data is transmitted from source to destination. Security is the most important factor in networks. There are possibilities to hack the wireless information. The hacking can be avoided with the help of Intrusion Detection Systems (IDS). Some protocols are used to determine the correct packets, here a new game theoretic approach is used to h increasing energy saving for sufficiently large, resource constrained networks. It proves to be a promising technology with Intrusion detection systems in WSN. In this paper we focus on the problem of WSN attacks & security using Honey pot technique

Keywords: WSN, IDS, Game Theory, Honey pot

I. INTRODUCTION

Wireless sensor networks are commonly used in pervasive and ubiquitous applications. WSNs are developed using both static (motes) and mobile (e.g. smart phone) sensor nodes for various applications such as smart homes, telehealth, surveillance, metering, and industry automation.

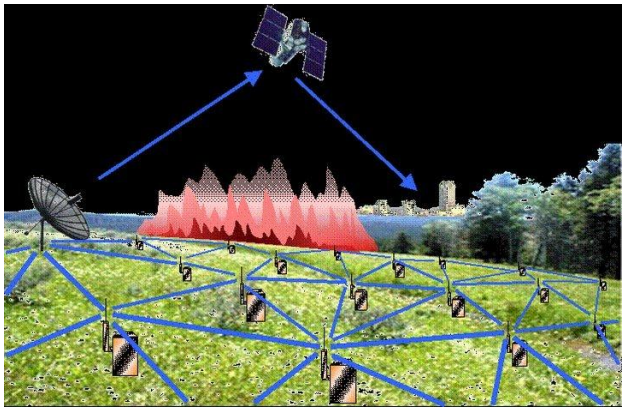

FIG 1.Wireless Sensor Network

The latest results and developments of WSN are under the following topics:

- Applications using mobile phones and static sensors
- Algorithms and techniques for energy efficient communication
- Robustness and fault tolerance in WSNs
- Intelligent techniques and data mining for WSNs
- Query processing for data streams in WSNs
- Security and privacy issues in WSNs
- Telehealth services for elderly and chronic patients using WSNs
- Body area sensor networks

Few limitations of WSN include computation, bandwidth, memory, and energy. Due to the hostile environments of WSNs, security is one of their most important aspects. IDSs are widely used for securing WSNs. IDS has the ability to detect an intrusion and raise an alarm for appropriate action. Due to the energy and computational power limitations, designing appropriate IDS for WSN is a challenging task.

Security attacks against WSNs

Security attacks against WSNs can be classified as active and passive [8, 9, 10]. Passive attacks are silent in nature and are conducted to extract important information from the network. Passive attacks do not harm the network or network resources. Active attacks are used to misdirect, temper, or drop packets. The unique characteristics such as wireless medium, contention-based medium access, multihop nature, decentralized architecture, and random deployment of such networks make them more vulnerable to security attacks at various layers.

IJCRCST © 2015 | All Rights Reserved

II.GAME THEORY

In general, game theory can be divided into two branches:

a) Non-cooperative and

b) Cooperative game theory.

a) Non-cooperative game theory

Non-cooperative game theory studies the strategic choices resulting from the interactions among competing players, where each player chooses its strategy independently for improving its own performance (utility) or reducing its losses (costs). For solving non-cooperative games, several concepts exist such as the celebrated Nash equilibrium.

b) Cooperative game theory

Cooperative game theory provides analytical tools to study the behavior of rational players when they cooperate. The main branch of cooperative games describes the formation of cooperating groups of players, referred to as coalitions [1] that can strengthen the players' positions in a game.

Application of non co-operative game theory

The mainstream of existing research in communication networks focused on using non-cooperative games in various applications such as

- Distributed resource allocation
- Congestion control
- Power control
- Spectrum sharing in cognitive radio, among others.

III. NEED FOR GAME THEORY IN WSN

The flexibility, fault tolerance, high sensing fidelity, low-cost and rapid deployment characteristics of WSNs are desirable features in creating many new and exciting application areas for remote sensing, detecting, tracking, and monitoring. However, it is non-trivial and very involved to design an optimal WSN to satisfy performance objectives such as maximum sensing coverage and extended operation periods. In order to obtain a practical and feasible WSN and due to the operation nature of the network, game theory (GT) is regarded as an attractive and suitable basis to accomplish the design goal. Game theory is a branch of mathematics and can be used to analyze system operations in decentralized and self-organizing networks. GT describes the behavior of players in a game. Players may be either cooperate or non-cooperative while striving to maximize their outcomes from the game. In this regard, sensors manage their operations in terms of power resources devoted to sensing and communicating among themselves and with a global controller such that the assigned task could be completed effectively as desired [4].

Cooperative game theory provides analytical tools to study the behavior of rational players when they cooperate and consider the utility of all the players [7, 8]. Non-cooperative game theory also covers a broad range of applications in WSN [9, 10]. In non-cooperative game theory, the nodes buy, sell, and consumer goods in response to the prices that are exhibited in a virtual market. A node attempts to maximize its profit for taking a series of actions. Whether or not a node receives a profit is decided by the success of the action. Note that non-cooperative game theory is mainly focused on each user's individual utility rather than the utility of the whole network. On the contrary, cooperative game theory can achieve general pare to-optimal performance and maximize the entire network's payoff while maintaining fairness. In addition to cooperative and non-cooperative game theories, repeated game theory is concerned with a class of dynamic games, in which a game is played for numerous times and the players can observe the outcome of the previous game before attending the next repetition [11]. The commonly used GT methods for solving WSN problems are listed in Table 1.

Table 1. Typical GT methods in WSN.

	Method
(1)	Cooperative game theory
(2)	Non-cooperative game theory
(3)	Repeated game theory
(4)	Coalitional game theory
(5)	Evolutionary game theory (extended)
(6)	Gur game
(7)	Bargaining game
(8)	Dynamic Bayesian game
(9)	TU game (transferable-utility game)
(10)	NTU game (non-transferable-utility game)
(11)	Ping-pong game
(12)	Zero-Sum game and Non-Zero-Sum game
(13)	Jamming game

IV. PROBLEMS OF GAME THEORY IN WSN

The problems that are identified from the survey includes:

S.NO	PAPER NAME	ABSTRACT	METHODS	DRAWBACK
1	**Game Strategies in Network Security**	Game theory is analyzing the security of distributed network. It makes an interconnection between attacker and administrator.	Stochastic game method, Non linear programming.	Nash equilibrium find between the both user and attacker is difficult.

2	**Incentive-BasedModellingandInferenceofAttackIntent,Objectives,andStrategies**	Objectivesand Strategies(AIOS)maydramaticallyadvancetheliteratureofriskassessment,harmprediction,andpredictiveorproactivecyberdefense,existingAIOSinferencetechniquesisadhoc	Attack Prediction, Game Theory, Computer Security	AIOSinference modelsbeyondBayesiangames
3	**Game-theoretic intrusion response and recovery**	Preserving the availability and integrity of networked computing systems in the face of those fast-spreading intrusions requires advances not only in detection algorithms, but also in intrusion tolerance.	Fictitious play, stochastic game theory	Securityincidents,suchasthetargetedStuxnetattackagainstnuclear power Plants, demonstratecurrentcomputersystems.
4	**Decentralized Intrusion Detection in Wireless Sensor Networks**	A distributed Rule based approach (interval rule)	Distributed: Scalable, robust and fast intrusion detection.	Rule based IDSs are simple to install and easy to operate. On the other hand, they need continuous rule updates in order to cope with the new released attacks
5	**Intrusion Detection in Sensor Networks: A Non-Cooperative Game Approach**	Hierarchical model with Game theory along with Markov decision process Only one of the clusters of the network is monitored at a time. This leaves the rest of the network un-protected	Markov decision process	clustering algorithms may consume considerable amount of the network's energy through the formation of the clusters. After the clusters are formed and the CHs are elected, CHs may constitute a single point of failure and they have to be secured. Besides, if the CH is not a special node (more powerful), then the overhead of being a CH will diminish its resources very quickly

Table 2.Literature Survey

V.EXISTING SOLUTIONS

To solve the security issues in WSN, there are several type of IDS have proposed. Such IDS techniques are as follows.

- Distributed and collaborative IDS
- Clustering (Hierarchical) based IDSs
- Game theory based IDSs
- Rule based IDSs
- Watchdog based IDSs
- Reputation (Trust) based IDSs

Drawbacks

In hierarchical, clustering based IDSs, clustering algorithms may consume considerable amount of the network's energy through the formation of the clusters. After the clusters are formed and the CHs are elected, CHs may constitute a single point of failure and they have to be secured. Besides, if the CH is not a special node (more powerful), then the overhead of being a CH will reduce its resources very quickly.

Agent based IDSs reduce the network load and latency. On the other hand, they cause high energy consumption of the nodes they are working on. Communication cost between agents and coordinator, or in between agents, may cause congestion and bottle neck in the network.

Rule based IDSs are simple to install and easy to operate. On the other hand, they need continuous rule updates in order to cope with the new released attacks. In game theory based IDSs, the detection rate can be adjusted by the network security administrator through changing the parameters. The problem with this system is that it is non-adaptive and requires human intervention for a stable operation.

VI. CONCLUSION

To resolve security issues & attacks in WSN many approaches has proposed. In future work, security issues and attacks will be minimized by using Honey pot technique in WSN than other approaches

IJCRCST © 2015 | All Rights Reserved

VII.REFERENCES

[1]. Y. Ping, J. Xinghao, W. Yue, and L. Ning, "Distributed intrusion detection for mobile ad hoc networks,"Journalof Systems Engineering and Electronics, vol. 19, no. 4, pp. 851–859, 2008

[2]. S. Northcutt and J. Novak, Network Intrusion Detection, SAMS, 3rd edition, 2002.

[3]. Sarvesh, V.; Gunes, E. On a Local Heuristic for a Reverse Multicast Forwarding Game.In*Proceedings of 2009 First International Conference on Networks & Communications*, Chennai,India, 27–29 December 2009.

[4]. Kazemeyni, F.; Johnsen, E.; Owe, O.; Balasingham, I. Group Selection by Nodes in WirelessSensor Networks Using Coalitional Game Theory. In *Proceedings of 2011 16th IEEEInternational Conference on Engineering of Complex Computer Systems (ICECCS 2011)*,Las Vegas, NV, USA, 27–29 April 2011.

[5]. Machado, R.; Tekinay, S. A survey of game-theoretic approaches in wireless sensor networks.*Comput.Netw.***2008**, *52*, 3047–3061.

[6]. Shen, S.; Yue, G.; Cao, Q.; Yu, F. A survey of game theory in wireless sensor networks security.*J. Netw*.**2011**, *6*, 521–532.

[7]. Saad, W.; Zhu, H.; Debbah, M.; Hjorungnes, A.; Basar, T. Coalitional game theory for communication networks: A tutorial. *IEEE Sign. Process. Mag*. **2009**, *26*, 77–97.

[8]. Fudenberg, D.; Tirole, J. *Game Theory*; MIT Press: Cambridge, MA, USA, 1991.

[9]. Krishnamurthy, V. Self-configuration in dense sensor networks via global games. *IEEE Trans. Sign. Process.***2008**, *56*, 4936–4950.

[10]. Krishnamurthy, V.; Maskery, M.; Yin, G. Decentralized activation in a ZigBee-enabled unattended ground sensor network: A correlated equilibrium game theoretic analysis. *IEEETrans. Sign. Process*.**2008**, *56*, 6086–6101.