STAR
Research Journal

Available online at www.starresearchjournal.com (Star International Journal)

ELECTRICAL ENGINEERING

UGC Journal No: 63023

Game Theoretic Modeling of WSN Jamming Attack and Detection Mechanism

S.Thiravida Arasi[1]

[1]*Research Scholar, Dept. of Computer Science, Dept. of Computer Science, Adaikalamatha College, Vallam, Thanjavur, (Affiliated to Bharathidasan University)*

Dr. L.Nagarajan[2]

[2]*Research Advisor, Director, Dept. of Computer Science, Adaikalamatha College, Vallam, Thanjavur, (Affiliated to Bharathidasan University)*

ABSTRACT:

A sensor network is a crucial network that is defined in a unique environment and with certain limitations. Security is always a major issue in these networks, just like it is in other networks. Network assaults come from both inside and outside. Jamming attack is one of these attacks. This assault happened as a result of extensive internal network node communication. The total criticality of the network also rises as a result of the network's increased energy consumption and load from intense communication. To find the secure network communication channel, a game theory adaptive model is defined in this study. Two primary phases make up the proposed model. According to the comparative study, the work has offered an energy-adaptive method for jamming infected networks.

INTRODUCTION

The idea of distributed architecture is provided via wireless networks, allowing for efficient resource and information exchange. The usage of sensor computers is growing quickly along with the development of the internet and personal computers. Several sensor nodes are connected to a large public area network, which is referred to as a sensor network [1]. The main characteristic of this type of network is mobility. Numerous nodes are communicated with using this type of network, which has multiple controller devices.

The choice of the next node is the primary WSN communication criterion. You can accomplish this in a static or dynamic manner. Maintaining a routing table can be used to provide static routing, while on-demand routing is referred to as dynamic routing. This type of routing starts with the source node and chooses the next neighbour node for communication after defining the coverage range. Repeat this procedure until the destination node does not arrive.

Ad-Hoc Network Types: In this case, the connection was built dynamically while creating a session. In order to draw effective communication through the system, the communicating device finds the other communicating device nearby while conducting the conversation. Until the target node is found, the search technique is used.

demand-based routing. This type of routing starts with the source node and chooses the next neighbour node for communication after defining the coverage range. Repeat this procedure until the destination node does not arrive.

Ad-Hoc Network Types: In this case, the connection was built dynamically while creating a session. In order to draw effective communication through the system, the communicating device finds the other communicating device nearby while conducting the conversation. Until the target node is found, the search technique is used.

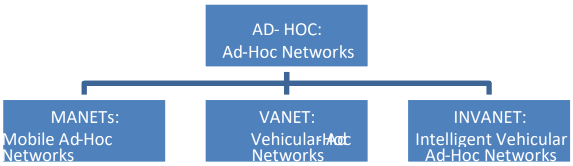

Figure 1: Types of Ad-Hoc Networks

The connection will be made using many nodes. Based on application domains, network circumstances, and configuration, several types of networks exist. In figure 1, these network kinds are listed.

Sensor Ad-Hoc Networks: A sensor network is an infrastructure-free network with sensors that connects to wireless devices in any topology and is automatically setup with the related hosts. In such networks, the topology might vary quickly, at random, or occasionally depending on the situation being employed. Figure 2 depicts the dynamic topology network in this case.

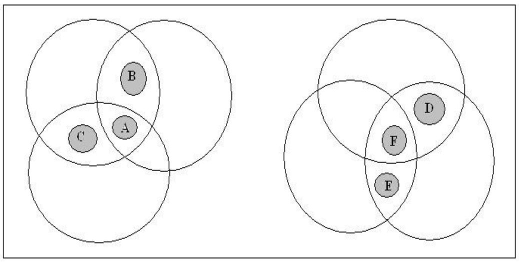

Figure 2: Ad-Hoc Networks Dynamic Topology

Vehicular Ad-Hoc Networks (Vanet): In VANET, another advanced type of sensor network, sensor devices are integrated into both roadside infrastructure and moving cars.

Intelligent Vehicular Ad-Hoc Networks (In-Vanet): It is a more advanced sort of vehicular network in which connected intelligent devices allow for inter-vehicle communication.

JAMMING ATTACK

In this attack, the malicious node falsely claims to have the fastest and most reliable route to the target, leading the other good nodes to choose this way through the malicious node. Once the route has been determined, the packets are either dropped or changed to contain routing updates. The routing procedure becomes unnecessarily complicated as a result [2]. There are two types of jamming attacks [3]:

Single JammingAttack: In a jamming attack, a rogue node just asserts that it has the shortest path while failing to send the packets after determining the route. In the network, a single jamming assault is easy possible [3]. This is seen in Figure 3.

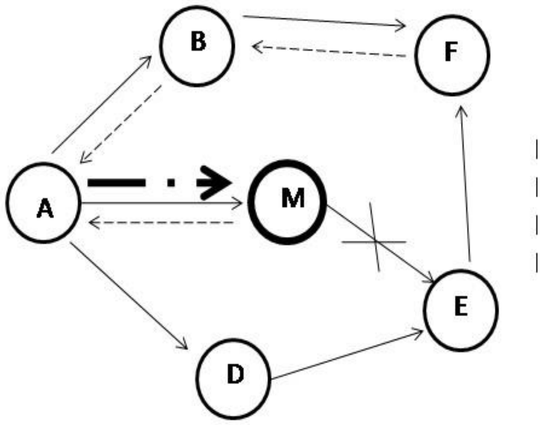

Figure 3: Single Jamming Attack

Cooperative Jamming Attack: A single node assault may involve many nodes working together, rendering them undetectable to other honest nodes [3]. In picture 4, the coordinated attack is depicted.

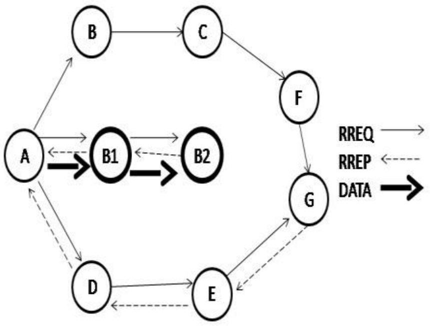

Figure 4: Cooperative Jamming Attack

IMPLEMENTATION ANAYLSIS

One essential type of ad hoc network where nodes cooperated to exchange information is a sensor network. But as a result of this cooperative behaviour, the network is vulnerable to several kinds of assaults. Jamming is one of these serious attacks. The purpose of the study that is being given is to offer a game theoretical model-based strategy for providing secure communication while under jamming assault. An method to constraint-specific behaviour analysis is defined in this study. Here, the task is divided into two key phases. The network will be separated into smaller sections in the first step, and behaviour related to constraints analysis will be carried out. The game theory-based constraint specific modelling will be created to identify the jamming assault once the crucial segments have been determined. Here, the election of the nodes and the accompanying communication analysis are carried out using a game theory technique. Here, the task is described as achieving complexity- adaptive network communication.

RESULTS

Matlab was used to implement the work that was presented.

Simulation Case Study: Here is a list of the simulation scenario settings for the study that was presented. Table 1: Simulation parameters

Parameter	Value
Area	200x200
Number of Nodes	100
Number of Rounds	100
Initial Energy	Random
Transmission Loss	5mJ
Receiving Loss	5mJ
Forwarding Loss	1 nJ
Topology	Random
Packet Drop Ratio	Random

Existing work (Results)

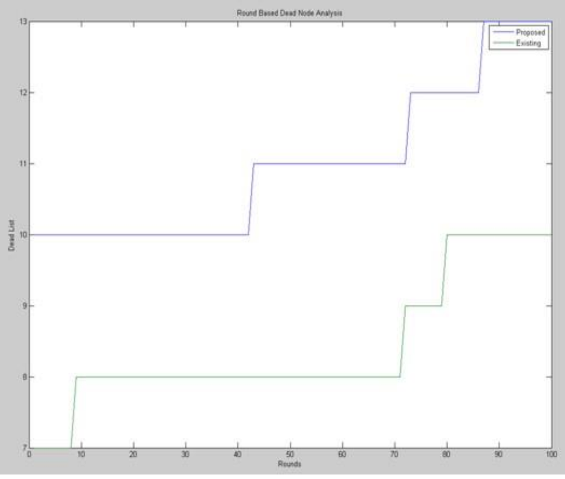

Figure 7 : Dead Node Analysis Analysis (Existing Vs. Proposed)

Figure 7 illustrates the examination of dead nodes for both current and projected work. The graphic demonstrates that there are more dead nodes in existing work than in proposed work. Because of this, planned work has a longer total network life than current work.

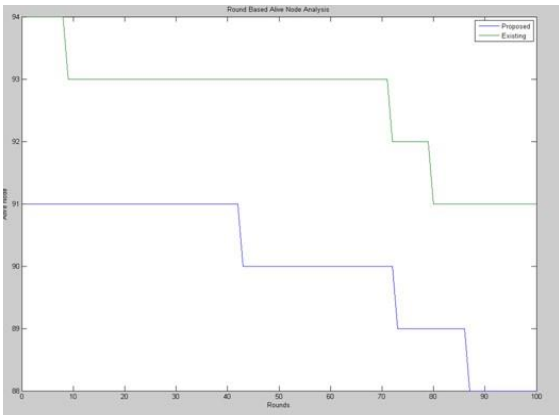

Figure 8 : Alive Node Analysis (Existing Vs. Proposed)

Here figure 8 is showing the alive node analysis in case of existing and proposed work. The figure shows that the alive nodes in existing work are lesser then proposed work. Because of this overall network life in case of proposed work is higher then existing work.

CONCLUSION

An efficient communication model under jamming assault is given in the current study. The provided model is based on the application of game theory. This concept is intended to enhance network longevity and communication efficiency. The network connectivity and life have both been enhanced by the suggested paradigm.

REFERENCES

1. H.R. Arabnia, A.N. Abbas, and G. Bebis, “Game theory for wireless sensor networks: A survey,” Computers & Electrical Engineering, vol. 41, pp. 1–20, 2015.
2. S. K. Das, C. Lin, and P. J. M. Havinga, “Game Theory in Wireless Sensor Networks: A Survey,” Mobile Networks and Applications, vol. 13, no. 6, pp. 683–702, Dec. 2008.
3. X. Wang, Z. Zeng, D. Xue, and Y. Li, “Game theory for wireless sensor networks: A survey,” International Journal of Ad Hoc and Ubiquitous Computing, vol. 19, no. 3, pp. 158–176, 2016.
4. S. Jiang, E. Hossain, and V. Bhargava, “Game Theory in Wireless Sensor Networks: A Tutorial,” IEEE Communications Surveys &

Tutorials, vol. 15, no. 2, pp. 676–697, Second Quarter 2013.

5. Z. Dong and P. Li, “Game theory applied to wireless sensor networks: a survey,” International Journal of Information and Electronics Engineering, vol. 5, no. 6, pp. 572–577, 2015.
6. Li, C., Li, X., Shi, Y., & Guizani, M. (2013). Game theoretic approaches for resource optimization in wireless sensor networks. IEEE Communications Surveys & Tutorials, 15(1), 320-335.
7. Chen, Y. C., & Huang, C. H. (2013). Networked control systems over wireless sensor networks: A game-theoretic approach. IEEE Transactions on Industrial Electronics, 60(1), 6-14.
8. Chatterjee, A., & Chakraborty, D. (2008). Game theoretic approaches for security in wireless sensor networks. IEEE Communications Surveys & Tutorials, 10(4), 60-72.
9. Koo, S. H., & Park, J. H. (2009). A game theoretic approach for secure data aggregation in wireless sensor networks. IEEE Transactions on Parallel and Distributed Systems, 20(5), 612-621.
10. Niyato, D., Wang, P., & Han, Z. (2008). Game theoretic models for optimization in wireless sensor networks. IEEE Wireless Communications, 15(3), 44-50.

11. Game Theory for Wireless Sensor Networks: A Survey by Hangyu Pei, Jie Wu, and Senior Member, IEEE, Qinghe Du
12. A Survey on Game Theory Applications for Wireless Sensor Networks by Muhammad Imran, Muhammad Zubair Khan, and Muhammad Naeem Khan
13. Game Theory for Wireless Sensor Networks: A Survey of Recent Advances by Kevin Chan, Member, IEEE, and Urbashi Mitra, Fellow, IEEE
14. A Survey on Game Theory Application in Wireless Sensor Network by Salma Khatun, and M. A. Kalam
15. Game-Theoretic Design of Wireless Sensor Networks by Zinan Lin, Member, IEEE, and Jie Wu, Senior Member, IEEE