Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 4, Issue. 6, June 2015, pg.648 – 653

RESEARCH ARTICLE

Game Theoretic Modeling of WSN Jamming Attack and Detection Mechanism

Ritu

R.N College of Engg. & Management, Rohtak (Haryana)

Ritu4648@gmail.com

Pooja Ahlawat

Asstt. Prof, CSE Deptt, R.N. College of Engineering and Management, Rohtak

Pooja.ahlawat5@gmail.com

Abstract: A sensor network is critical network for defined in specialized scenario and with restricted constraints. As of other networks, security is always the critical challenge in these network. The network suffers from internal and external attacks. One of such attack includes jamming attack. This attack occur because of high communication in the network performed by internal network nodes. As the heavy communication increases the energy consumption and load in the network, the overall criticality of network also increases. In this research, a game theory adaptive model is defined to identify the safe communication path over the network. The presented model is divided in two main stages. The comparative analysis shows that the work has provided the energy adaptive solution in jamming infected network.

I. INTRODUCTION

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[1] is defined as a wide public area network in which number of sensor nodes are connected. Mobility is the key property of such kind of network. These kind of networks performs the communication with multiple nodes under multiple controller devices.

The main communicating criteria of WSN is 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.

Types of Ad-Hoc Networks: The connection is here been established dynamically while defining a session. While performing the communication, the communicating device discovers the other communicating device in the range so that effective communication will be drawn over the system. The search mechanism is performed till the target node is not identified.

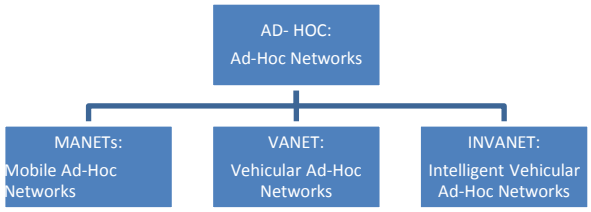

Figure 1: Types of Ad-Hoc Networks

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.

Sensor Ad-Hoc Networks: A Sensor network is the infrastructure less network with sensor network that is configured automatically with the associated hosts and connected to the wireless devices in the form of arbitrary topology. The topology in such network change rapidly and on random basis or some times on the basis of the scenario used in the work. Here figure 2 is showing the dynamic topology network.

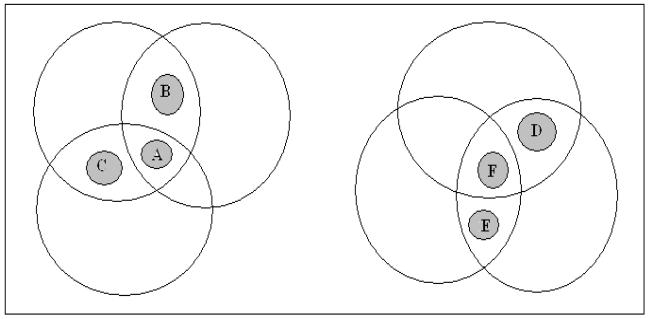

Figure 2: Ad-Hoc Networks Dynamic Topology

Vehicular Ad-Hoc Networks (Vanet): VANET is the another advance form of sensor network in which the sensor devices are incorporated in the vehicles as well as in road side equipments.

Intelligent Vehicular Ad-Hoc Networks (In-Vanet): It is the improved form of vehicular network in which intelligent devices are connected to enable the communication among the vehicles.

II. JAMMING ATTACK

In this attack, the malicious node advertises fake routing information such as it has the shortest and stable path to reach the destination, and causes the other good nodes to establish the path through this malicious node. Once the path is established, then it either drops the data packets, or changes the routing updates packets. This creates unnecessary confusion in the routing process [2]. Jamming attack can be of two types [3]:

Single JammingAttack:A Jamming attack simply means a malicious node claims itself as having the shortest path, but it does not forward the packets after establishing the route. A single jamming attack can easily happen in the network [3]. This is shown in the figure 3.

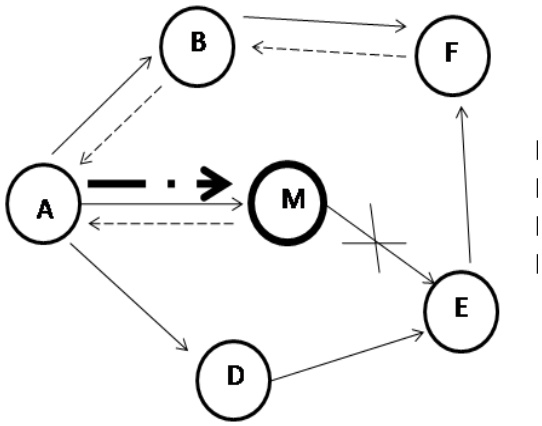

Figure 3: Single Jamming Attack

Cooperative Jamming Attack: There can be more than one node which is cooperating with the single node attack making them invisible from the other honest nodes [3]. The cooperative attack is shown in figure 4.

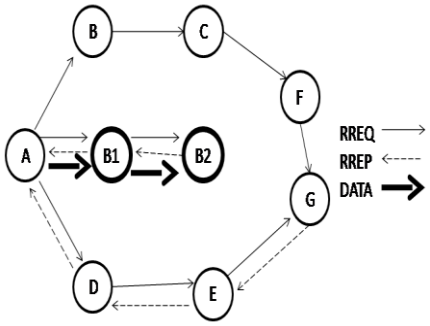

Figure 4: Cooperative Jamming Attack

III. IMPLEMENTATION ANAYLSIS

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 behaviour 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. The flow of presented work is given here under

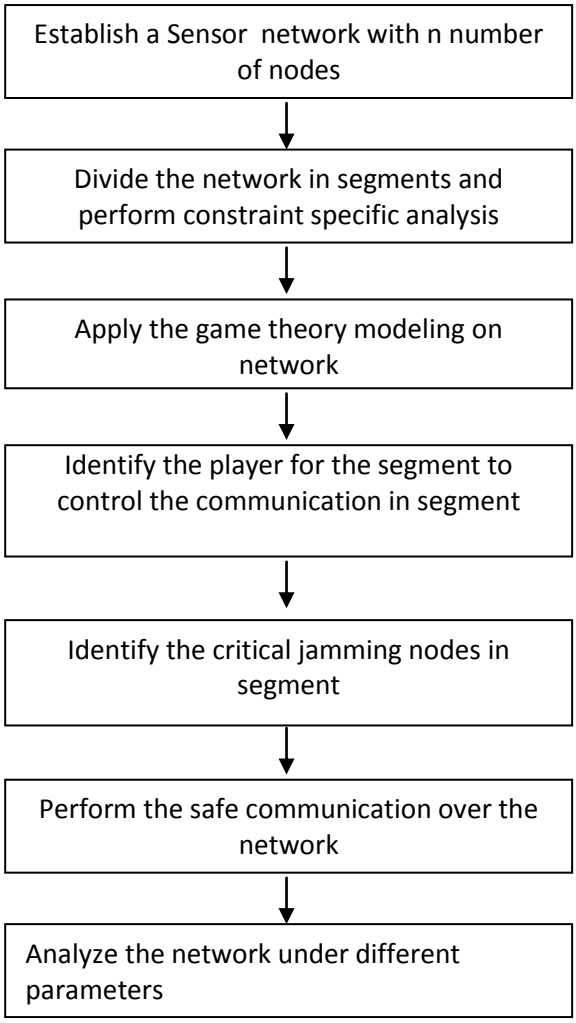

Figure 5 : Work Model

Here figure shows that the work has provided the effective and reliable communication over the sensor network.

The game theory approach is here applied to perform the election of the nodes and the communication analysis in associated form. The work is here defined to achieve the complexity adaptive communication over the network..

IV. RESULTS

The presented work is implemented in matlab.

Simulation Scenario: The simulation scenario parameters of presented work are listed here under

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)

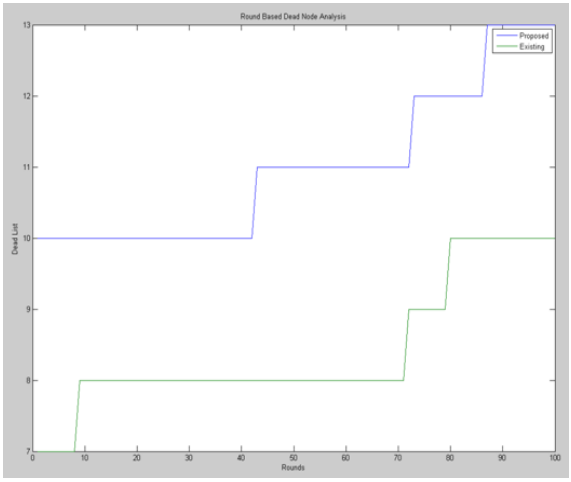

Figure 7 : Dead Node Analysis Analysis (Existing Vs. Proposed)

Here figure 7 is showing the dead node analysis in case of existing and proposed work. The figure shows that the dead nodes in existing work are higher then proposed work. Because of this overall network life in case of proposed work is higher then existing work.

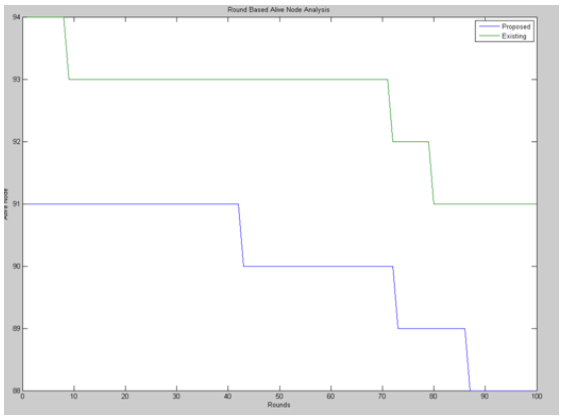

Figure 8 : Alive Node Analysis (Existing Vs. Proposed)

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.

V. CONCLUSION

In this present work, an effective communication model is presented under jamming attack. The presented model is based on the game theory approach This model is defined to optimize the network communication and to improve the network life. The proposed model has improved the network communication and network life.

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] Yuanyuan Zeng, "Joint Power Control, Scheduling and Real-time Routing in Wireless Sensor Networks", International Conference on Advance Computer Control, pp 357-361, 2010.

[3] Feng Liu, "Joint Routing and Sleep Scheduling for Lifetime Maximization of Wireless Sensor Networks", IEEE Transactions on Wireless Communications, pp 2258-2267, 2010.

[4] Yu Gu, "Joint Scheduling and Routing for Lifetime Elongation in Surveillance Sensor Networks", IEEE Asia-Pacific Services Computing Conference, pp 81-88, 2007.

[5] Saeyoung Ahn, "Slotted Beacon Scheduling Using ZigBee Cskip Mechanism", The Second International Conference on Sensor Technologies and , pp 103-108, 2008.

[6] 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.

[7] 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.

[8] Chunsheng Zhu, "Sleep Scheduling Towards Geographic Routing in Duty-Cycled Sensor Networks", International Conference on Distributed Computing and Workshops, pp 1-3, 2011.

[9] 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.

