International Journal of Enhanced Research in Management & Computer Applications
ISSN: 2319-7471, Vol. 6 Issue 2, February-2017, Impact Factor: 1.544

Mechanism Study of Wireless Sensor Network Jamming Attack and its Detection

Asha Rani

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

ABSTRACT

The jammer action ceases when it is detected by a monitoring node in the network, and a notification message is transferred out of the jamming region. The jammer is detected at a monitor node by employing an optimal detection test based on the percentage of incurred collisions. In order for the jammer to optimize its benefit, it needs to know the network channel access probability and number of neighbors of the monitor node. 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 this network. The network suffers from internal and external attacks. One of such attack includes jamming attack. This attack occurs 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.

Keywords: E-commerce, WSN, jamming, attack,

1. INTRODUCTION

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 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 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.

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.

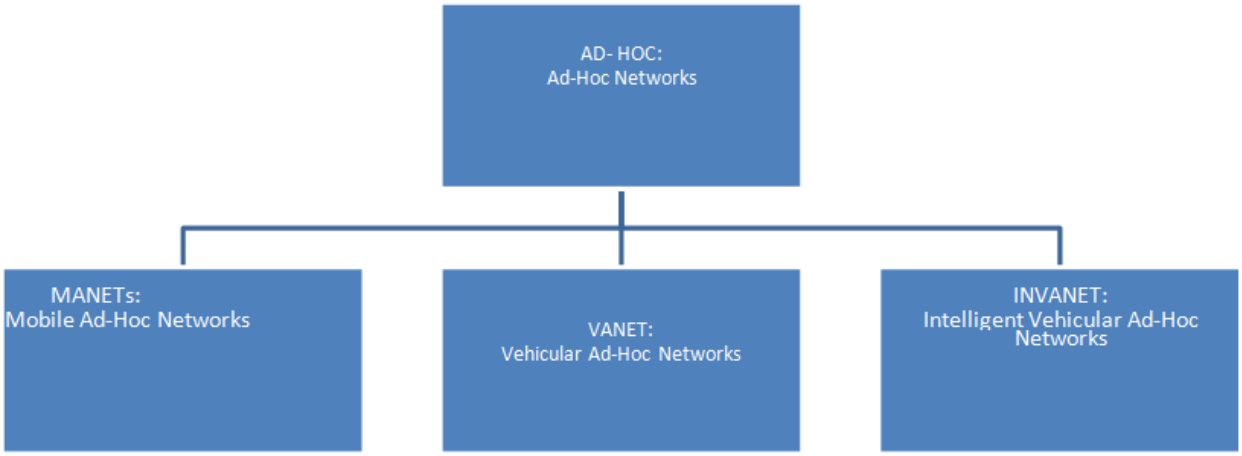

Fig. 1: Types of Ad-Hoc Networks

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.

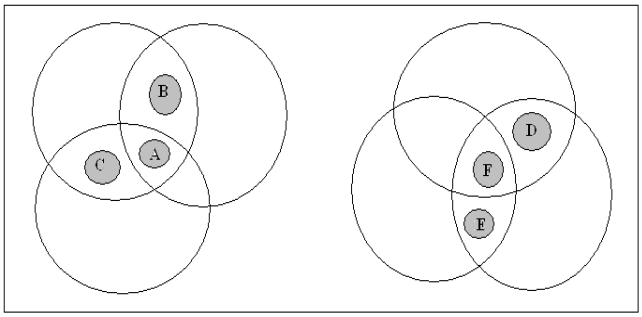

Figure 2: Ad-Hoc Networks Dynamic Topology

Vehicular Ad-Hoc Networks (Vanet): VANET is the 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.

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].

For the communication of jamming attack there are three ways are available : jamming passive resistance , jamming revelation, jamming extenuation. The equable and adequate way in order to avoid the jammer is to moving out of the jamming region and by interchange the communication link and the packet cannot be affected by the jammer. Instead of the jammer adequateness, the most of jammer is never possible in most of the wireless application . 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 reduces. Jamming attack can be of two types [3]:

Single Jamming Attack: 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.

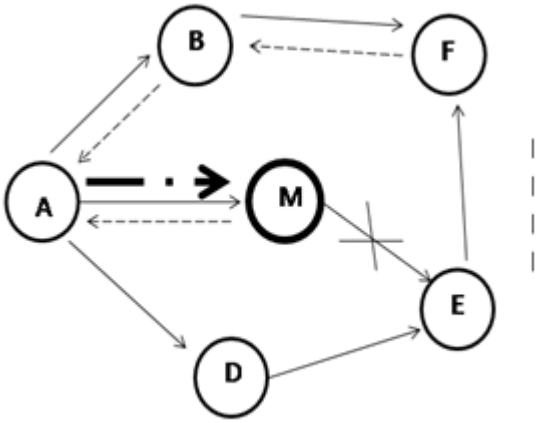

Figure 3: Single Jamming Attack

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.

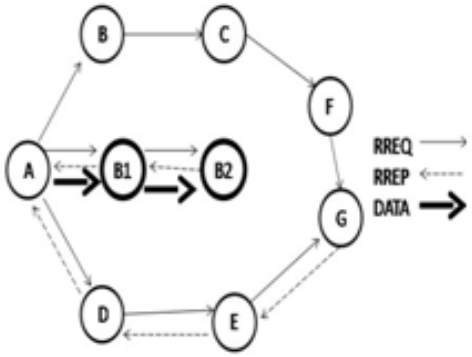

Figure 4: Cooperative Jamming Attack

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. The flow of presented work is given here under :

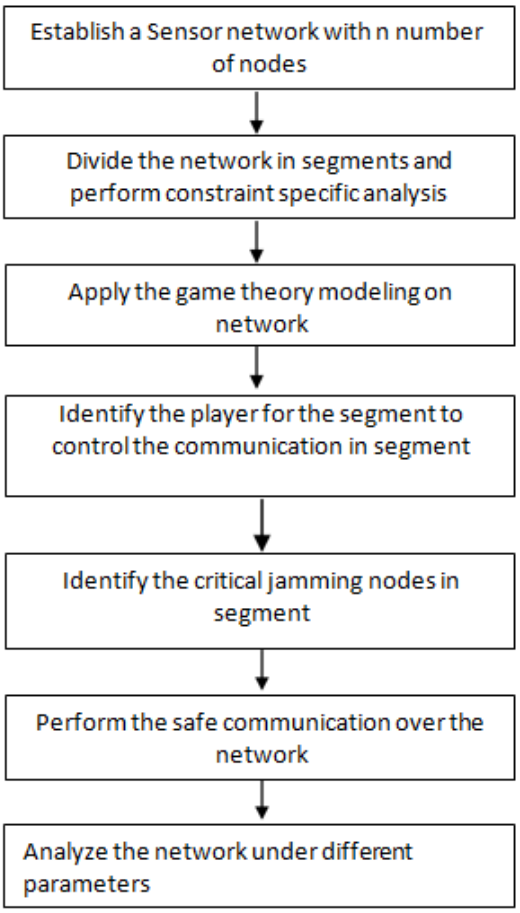

Figure 5: effective and reliable communication

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..

RESULTS

The presented work is implemented in matlab.
Simulation Scenario: The simulation scenario parameters of presented work are listed here under:

Table 1: Simulation Scenario 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

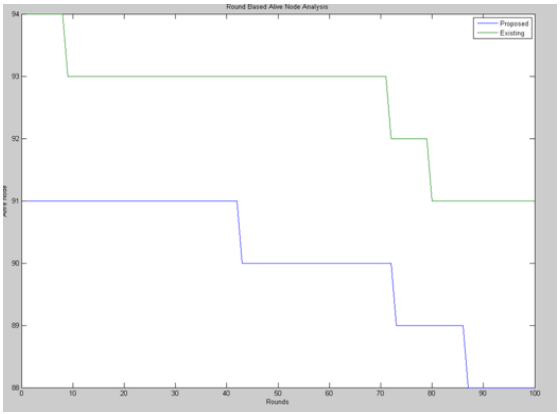

Figure 6: Alive Node Analysis

Here figure 6 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 than existing work.

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]. 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.