International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 04 Issue: 03 | Mar -2017 www.irjet.net p-ISSN: 2395-0072

A Survey Paper on Jamming Attacks and its Countermeasures in Wireless Networks

Chaithra H S[1], Rashmi B[2], Johnpaul C I[3]

[1]*B.E. in Information Science and Engineering, NIE, Mysuru, Karnataka, India*

[2]*B.E. in Information Science and ENGINNERING, NIE, Mysuru, Karnataka, India*

[3]*Assistant Professor, Department of Science and Engineering, NIE, Mysuru, Karnataka, India*

Abstract - *In a wireless networks communication between events uses logical communication channels i.e. the timing channel in which the information is encoded in timing. The use of timing channel has been proposed to defeat reactive jamming attacks; timing information cannot be jammed even though the attacker can destroy the contents of the packets. Since the target node and the jammer have conflicting interests, Game Theory is used to model the interactions between them. In this paper we analyze the interactions between the jammer and the target node using Game Theoretic Model. In game theory, the Nash equilibrium is a solution control of a non-cooperative game. In a network all communication nodes will set their own strategies and the reactions of the jammer will be according to the nodes strategies. This is been analyzed and modeled as a Stackelberg Game. The numerical results obtained are presented, which shows the system performance which is based on network parameters like bandwidth, delay etc.*

***Key Words*: Game Theoretic Model, Stackelberg Game, Nash Equilibrium.**

1. INTRODUCTION

In wireless networks transferring of any kind of information between one or more nodes takes place that are not physically connected. Because of its shared medium and broadcast nature, wireless networks are prone to various kinds of attacks. This leads to numerous security issues which need to be dealt. The communication in the network can be disturbed by many attacks strategies. Denial of service attack is one of the effective attacks on wireless network. Jamming attack comes under DOS attack [1]. Fundamental way of degrading network performance is by using jamming. Jamming is one of many exploits used to compromise the wireless environment. Its works by denying service to authorize users as legitimate traffic is jammed by the overwhelming frequencies of illegitimate traffic [2]. Two forms of jamming exist, they are

- External threat model: Jammer is not part of the network.
- Internal threat model: Jammer is the part of network.

Wireless transmission can be disrupted by jamming either in the form of interference noise or collision at the receiving node. It lowers the signal–to- noise ratio by injecting high level of noise to the transmitted signals. An ideal jamming attack should have less chance of being detected, energy efficient, resistant to anti jamming techniques and also it should disrupt the communication to maximum possible extent.

2. ANALYSIS OF JAMMING ATTACKS

Communication security is associated with two features, reliability of the system. Secret message transmission to a valid receiver under certain conditions is called as message secrecy. If the intended message is reliably received by that receiver node is known as system reliability. Jammer is the threat to system reliability. Categories of Jamming attacks are:

2.1. Active and Passive attacks

Passive attackers do not transmit any message; it just monitors the channel and tries to steal the packet containing IP addresses and other node related information. It does not cause any direct damage to the communication network it just steals the information which can be misused which causes a threat to network confidentiality. Active attackers make the network to malfunction which affects the normal operation of the specific node. Active attacker performs dropping of packets, deleting packets to wrong destination

which violate non-repudiation, integrity, availability and authentication.

2.2. Internal and External attacks

In internal attacks jammer is part of the network to disrupt the network communication.

In external attacks jammer is not part of the network [6].

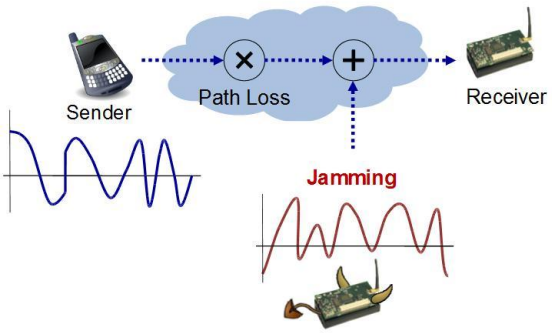

Fig 1. Jamming attack in wireless network

3. DIFFERENT ANTI-JAMMING TECHNIQUES

In order to recover from jamming attack efficient prevention mechanism is required. Prevention approaches are more important in wireless network because they provide an efficient approach to increase the network performance. Existing jamming prevention techniques are wavelength assignment, Channel surfing, Game theory approach, Zonalization, Trigger identification, Frequency hopping, Threshold based technique, Cryptographic key distribution, Multi path routing, Packet hiding

3.1. Wavelength assignment

Network performance is degraded by high powered jamming attack which must be dealt efficiently. Most of the challenges that exist in preventing jamming attack are successfully solved using routing and wavelength assignment. Different techniques of wavelength assignment are:

- Attack aware routing and wavelength assignment
- Attack-Aware Wavelength Assignment
- Maximum Light Path Attack Radius

3.2. Channel surfing

It is an effective method to prevent jamming attack in wireless network. Negotiation takes place between two parties as a result to agree upon the channel switching sequence beforehand. Different techniques of channel surfing's are:

- Neighbour based proactive channel hopping
- Channel surfing without prior Negotiation
- Defence using Honey nodes and channel surfing algorithms
- Adaptive rapid channel hopping

3.3. Game theory approach

Zero sum stochastic game is modelled between secondary use SU and attackers. For transmitting control messages from time to time multiple channels are reserved according to attacker's strategy. For maximising the payoff function secondary users avoid jamming attack by proactively hopping among accessible channels. Different techniques of game theory approach are:

- Stochastic Anti-Jamming Game Formulation
- Anti-Jamming Channel Hopping Game
- To Hop Or Not To Hop
- Game-theoretical Anti-Jamming

3.4. Frequency hopping

The frequency bands on which the signals are transmitted are changed by the transmitter. The spectrum for the communication system is divided into a number of frequency band and time slots are obtained by dividing the time. Spreading code is got by assigning each user with a frequency hopping pattern. Different techniques of frequency hopping are:

- Code tree based system
- Time-Delayed Broadcast
- Uncoordinated Spread Spectrum

3.5. Multipath routing

The source and the destination are provided with end-to-end availability for multi paths which is known as multipath availability. It identifies the reliable path for data

transmission. Different techniques of multipath routing are:

- Jamming-Aware Source Routing
- Availability History Vectors Algorithm Based on Multipath Routing

3.6. Threshold based

Jamming caused by jamming signal can be mitigated by using threshold based schemes. The data are transmitted based on the threshold value maintained by each node in the network. Different techniques of threshold based are:

- Multi-packet transmission(MPT) and Multi-packet reception(MPR)
- ANTIJAM MAC protocol

3.7. Cryptographic key distribution

Security is provided against jamming attack by providing cryptographic keys to nodes. Encrypting every packet is the solution, so that the jammer will not be able to figure out the packet. The number of keys depends on the number of nodes. Secret key assignment to all pair of node is difficult. The solution is to assign the keys randomly and connect each other. Different techniques of cryptographic key distribution are:

- Hybrid key pre-distribution
- Greedy user IDEntification Algorithm

3.8. Hiding scheme

Contextual information such as traffic data are hid from attackers using hiding schemes. Hiding can be done using fake data source or between layers. Different techniques of hiding schemes are:

- Packet hiding scheme
- Hiding Traffic with camouflage
- Resource-efficient hiding

4. GAME THEORETIC APPROACH

The objective of the wireless networks is to safely transfer the packets received from the source to the destination. The objective of the jammer will be, to cause significant network disruption using sophisticated strategies to avoid detection which would otherwise truncate the attack duration. Similarly the wireless network may choose to modify the communication system in order to avoid interference from the jamming transmission and to improve overall performance in the presence of jamming. Since there is a conflict between the interest of the jammer and the nodes under attack. So we model this conflict using Game Theory.

4.1. Game Formulation

To model the interaction between the wireless network and the jamming node, we set up a two player jamming game. At a given instant, the jamming node and the node under the attack choose a strategy to execute and obtain certain payoff based on the chosen strategies. The strategies chosen by the jamming node and the network is given by the pair $r_{ij} = (r_i, r_j)$ in the set $R=R_i \times R_j$. Each pair r_{ij} has its own associated pros and cons. Payoff function combines the benefits associated with strategy chosen and the effects of the strategy proposed by the opponent i.e $P_j(r_{ij})$ for the network and $P_j(r_{ij})$ for the jammer. For Example the jammer chooses the strategy i.e no jamming activity (r_j) and the network chooses the strategy to mitigate jamming attack (r_i). In this case, $P_j(r_{ij})=0$ because no resource are used and there is no chances of detection, while $P_i(r_{ij})<0$ because resources are used with no benefit. The dynamic nature of the interaction between the jammer and the network makes it possible for both players to continually modify their strategies. So a repeated game is considered which consists of number of sub games corresponding to the strategies r_i and r_j. In a given sub game, each player's aim is to choose the strategy r_i^* or r_j^* which maximises the payoff $P_j(r_{ij})$ or $P_i(r_{ij})$. For a specific sub game a strategy $r^*=(r_i^*, r_j^*)$ is said to be a Nash Equilibrium[8] for that sub game if neither one of the players can increment their payoff by going amiss from their present strategy. For example, if $P_j(r^*)=4$ and $P_i(r^*)=2$ is a Nash Equilibrium for the sub game, then $P_j(r_j, r_i^*)<=4$ for all $r_j \in R_j$ and $P_j(r_j^*, r_i)<=2$ for all $r_i \in R_i$. At the end of the day, NE relates to every player's best reaction to their opponent's moves. Furthermore, the presence of NE is ensured for any game, potentially including probabilistic strategies [7].

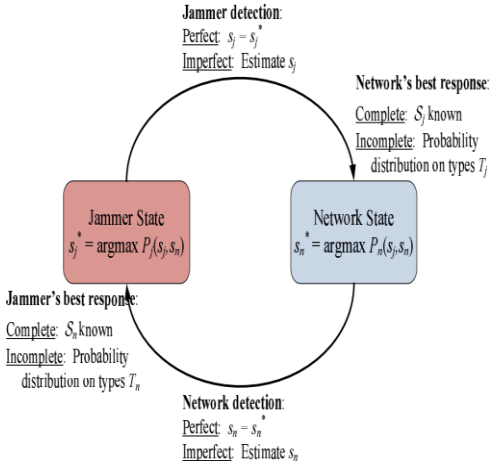

Fig 2. Interaction between network and jammers

[5] In the above diagram we have used s_n and s_j as r_i and r_j (strategies of network and jammer) respectively. The communication between the network and jammers is illustrated as a block diagram, demonstrating that each of the network's and jammer's techniques is picked in view of the opponent's already used strategies.

5. CONCLUSION

In this paper we have studied about the timing channel, jamming, and the security issues that arise because of jamming in wireless network. We have mentioned about different jamming methods, in which Reactive jamming appears to be the effective jamming method which is difficult to detect. In this paper we have also given an outline about different anti- jamming techniques. We have proposed a game theoretic framework to resolve the conflicting interests between the network and the jammer.

REFERENCES

[1] www.spamlaws.com

[2] S. Raja Ratna, R. Ravi- Survey on jamming Wireless networks: Attacks and prevention strategies world academy of science.

[3] Engineering and Technology, International journal of computer, Electrical, Automation, Control and Information Engineering, vol: 9, NO: 2, 2015

[4] Neha Takur and Arun Sankaralingam introduction to jamming attacks and prevention techniques using honeypots in wireless networks, ORACST-International journal of computer science [IJCSITS], ISSN:2249-9555, vol:3, NO:2, April 2013

[5] David Slater, Patrick Tague, Radha Poovendran, A Game Theoretic framework for jamming attacks and Mitigation in commercial aircraft wireless networks.

[6] Mobile, embedded and wireless security.

[7] C.Gowdham1, E.Praveen2, B.Gari Gabreil, A Game Theoretical Analysis of Exploiting Timing Channels to overcome Jamming.

[8] Fudenberg, D. and Tirole, J.,Game Theory, MIT Press, 1991.