Scientific Journal of Impact Factor (SJIF): 4.14

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 3, Issue 12, December -2016

Detecting Jamming Using RTS CTS Strategy

[1]Anita Wakode, [2]Mayuri Halnor, [3]Rashmi Singh, [4]Prof.Aditi Chaturvedi

[1,2,3,4] *Department of Computer Engineering, JSPM Pune*

Abstract--- *Time-critical wireless applications in rising network systems, like healthcare and sensible grids, are drawing increasing attention in each business and academe. The printed nature of wireless channels inescapably exposes such applications to electronic jamming attacks. However, existing strategies to characterize and notice electronic jamming attacks cannot be applied on to time-critical networks whose communication traffic model differs from standard models. In this paper we recommend a brand new category of anti-jamming issues wherever the kind of intelligence associated with an electronic jamming attack is unknown. Specifically, we tend to take into account a problem wherever the nodes of a peer-to-peer network don't grasp whether or not the network is under fire by a random sender (which may well be thought of as a natural background noise), or associate degree intelligent one (i.e., the sender UN agency will adapt his strategy supported data gained throughout attacks). The goal of the nodes is to identify the kind of the attack supported data obtained from the attack in previous time slots, and thereby to cut back the potency of the electronic jamming attack. First we tend to model the matter as a theorem game for one slot attack, and reduce it to the answer of twin applied math (LP) issues.*

Keywords *- Rate Adaptation, Anti Jamming, P2P, LP, Experimentation.*

I. INTRODUCTION

Mobile unexpected network (MANET) falls within the class of wireless unexpected network, and could be a self-configuring network. Every device is absolved to move severally in any direction, and therefore can modification its link with different devices oftentimes. Every node should forward traffic that isn't associated with its own use, and so be each a router and a receiver. This feature conjointly comes with a significant disadvantage from the protection purpose of read. Certainly, the above-named applications impose some severe constraints on the protection of the constellation, routing, and information traffic. As an example, the existence and collaboration of malicious nodes within the network might disturb the routing method, resulting in a faulty of the network operations. The protection of MANETs deals with bar and detection strategies to struggle individual misbehaving nodes. With relevancy the effectiveness of those strategies becomes weak once multiple malicious nodes conspire along to initiate a cooperative attack, which may result to a lot of stunning damages to the network. These networks square measure extremely liable to routing attacks like black hole and gray hole (known as variants of black hole attacks).

II. LITERATURE SURVEY

2.1 Paper Name: Peer-to-peer group *k*nearest neighbours in mobile ad hoc networks

Authors: T.P. Nghiem, D. Green, and D. Taniar

Description: The increasing use of location-based services has raised several problems with call support and resource allocation. an important downside is the way to solve queries of cluster k-Nearest Neighbour (GkNN). A typical example of a GkNN question is finding one or several nearest meeting places for a gaggle of individuals. Existing strategies principally admit a centralized base station. However, mobile P2P systems supply several edges, as well as self-organization, fault-tolerance and load-balancing. during this study, we have a tendency to propose and measure a completely unique P2P algorithmic rule that specialize in GkNN queries, during which mobile question objects and static objects of interest area unit of 2 totally different classes. The algorithmic rule is evaluated within the MiXiM simulation framework with each real and artificial datasets. The results show the sensible practicableness of the P2P approach for resolution GkNN queries for mobile networks.

2.2 Paper Name: Incorporating attack-type uncertainty into network protection

Authors: A. Garnaev, M. Baykal-Gursoy, and H.V. Poor

Description: Network security against doable attacks involves creating selections beneath uncertainty. Not solely might one be unaware of the place, the power, or the time of potential attacks, one might also be for the most part unaware of the attacker's purpose. for example this development, this paper proposes a straightforward theorem game-theoretic model of allocating defensive (scanning) effort among nodes of a network during which a network's defender doesn't apprehend the adversary's motivation for intrusive on the network, e.g., to bring the largest harm to the network (for example, to steal master card numbers or data on bank accounts hold on there) or to infiltrate the network for alternative functions (for example, to corrupt nodes for an extra distributed denial of service botnet attack on servers).

2.3 Paper Name: Jamming Games for Power Controlled Medium Access with Dynamic Traffic
Authors: Yalin Evren Sagduyu, Randall A. Berry, Anthony Ephremides
Description: Due to the published nature of the wireless medium, wireless networks are extremely prone to ECM attacks. Such attacks are usually studied in a very game theory-based framework beneath the idea of uninterrupted traffic subject to continuous ECM opportunities. Instead, we tend to analyze the result of dynamically dynamic traffic on ECM games for power controlled medium access. Random packet arrivals raise the chance that the transmitter queues could also be empty once ECM attacks begin and so waste the energy of jammers. We tend to contemplate a non-cooperative game during which transmitters and jammers choose their transmission power to balance the transmission value subject to delay and energy constraints. We tend to show that jammers incur a major performance loss once they don't have data of transmitter queue states. Dynamic traffic will increase the immunity to ECM attacks and provides insights into defense mechanisms.

III. PROPOSED SYSTEM

We develop a gambling primarily based model to derive the message breakup quantitative relation of the time-critical application below ECM attacks. We have a tendency to established time period experiments to validate our associate analysis and more evaluate the impact of ECM attacks on an experimental power station network. Supported our theoretical and experimental results.

We style and implement the system named opposing jamming electronic ECM jam electronic countermeasures ECM on Estimation to realize economical and reliable jamming detection for power networks.

Advantage of Proposed System:

1. The system achieves economical and sturdy ECM detection for power networks.
2. This system is reliable.
3. It is a lot of applicable than typical performance metrics for time-critical applications.

IV. SYSTEM ARCHITECTURE

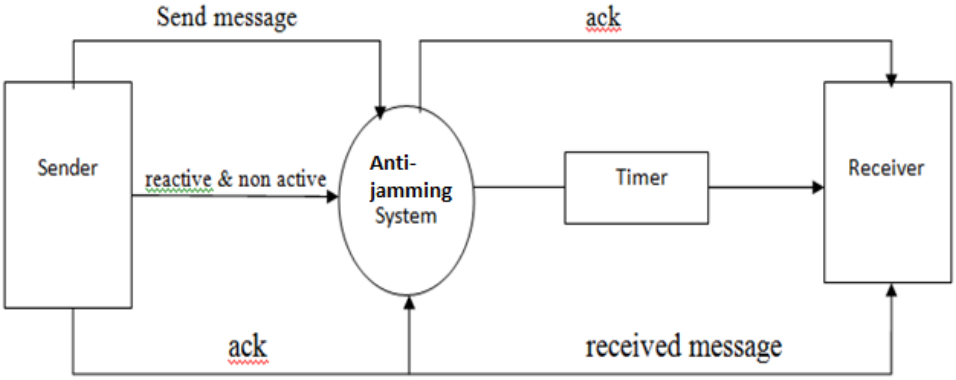

Figure 1. Architecture Diagram of Proposed System

V. MATHEMATICAL MODEL

Let W be the whole system which consists:
W = {input, process, output}.

Input: {p, N, F,}.
Where,

1. p probability of jamming.
2. N is number of samples taken for estimation.
3. F is the frequency of number of jamming events.

Process:
We implement the anti jamming system that periodically transmits raw data samples at the rate of 920Hz. Our system observes the transmission result of each data sample and estimates the jamming probability p` by

$$\mathrm{P`} = \frac{1}{N}\sum_{i=1}^{N} 1_{F_i}$$

Where N is the number of observations jamming attacks in the network, and Fi denotes the event that the i-th transmission fails.
After the estimation in, the anti jamming raises a jamming alarm if p` > p∗.

VI. CONCLUSION

In this paper, we tend to provide an in-depth study on the impact of jam attacks against time-critical sensible grid applications by theoretical modeling and system experiments. We tend to introduce a metric, message breakup magnitude relation, to quantify the impact of jam attacks. We tend to showed via each analytical analysis and period experiments that there exist state change phenomena in time-critical applications beneath a range of jam attacks. Supported our analysis and experiments, we tend to designed the anti -system to realize economical and strong jam detection for power networks.

REFERENCES

[1] T.P. Nghiem, D. Green, and D. Taniar, "Peer-to-peer group *k*nearestneighbours in mobile ad hoc networks," in *Proc. 19th IEEE International Conference on Parallel and DistributedSystem*, pp. 166–173, 2013.

[2] H. Yang, H.Y. Luo, F. Ye, S.W. Lu, and L. Zhang, "Securityin mobile ad hoc networks: challenges and solutions," *IEEEWireless Communications*, vol. 11, pp. 38–47, 2004.

[3] R.A. Poisel, *Modern communications jamming principles andtechniques*. London, Boston: Artech House Publishers, 2006.

[4] W. Xu, W. Trappe, Y. Zhang, and T. Wood, "The feasibility oflaunching and detecting jamming attacks in wireless networks,"in *Proc. the 6th ACM international symposium on Mobile ad hocnetworking and computing (MobiHoc)*, pp. 46–57, ACM Press,2005.

[5] R. Negi and S. Goel, "Secret communication using artificialnoise," in *Proc. IEEE 62nd Vehicular Technology Conference(VTC-2005-Fall)*, vol. 3, pp. 1906–1910, 2005.

[6] W. Xu, "Jamming attack defense," in *Encyclopedia of cryptographyand security* (H.C.A Tilborg and S. Jajodia, eds.), pp. 655–661, NY: Springer, 2011.

[7] Y. Wu, B. Wang, K.J.R. Liu, and T.C. Clancy, "Anti-jamminggames in multi-channel cognitive radio networks," *IEEE Journalon Selected Areas in Communications*, vol. 30, pp. 4–15, 2012.

[8] Y.E. Sagduyu, R.A. Berry, and A. Ephremides, "Jamminggames for power controlled medium access with dynamic traffic,"in *Proc. IEEE International Symposium on InformationTheory Proceedings (ISIT)*, pp. 1818–1822, 2010.

[9] D. Fudenberg and J. Tirole, *Game theory*. MIT Press, 1991.

[10] M.H. Manshaei, Q. Zhu, T. Alpcan, T. Basar, and J.-P. Hubaux,"Game theory meets network security and privacy," *ACM ComputingSurvey*, vol. 45, no. 3, 2013.

