IJRRECS/October 2013/Volume-1/Issue-6/1035-1040 **ISSN 2321-5461**

**INTERNATIONAL JOURNAL OF REVIEWS ON RECENT ELECTRONICS AND COMPUTER SCIENCE**

# AUTOMATIC SENSING OF JAMMING ATTACKS IN DYNAMIC WIRELESS AD HOC NETWORKS

**Mohammad Arif C[1], Naveen Immadi[2]**

**[1]M.Tech Student, Dept of CSE, Aurora's Technological and Research Institute, Parvathapur, Uppal, Hyderabad, A.P, India**

**[2]Associate Professor, Dept of CSE, Aurora's Technological and Research Institute, Parvathapur, Uppal, Hyderabad, A.P, India**

**ABSTRACT:**

Attacks related to the international interference which plays a major frustration towards the system and is one of the vulnerable problems for the system oriented with the network of the wireless phenomena is an open problem well arising in the society based aspects respectively. And these types of the attacks are considered as the attacks of the jamming are a primary concern respectively. Here the transmission of the data in the wireless analysis by which related to the interference of the international phenomena oriented with the problems of the service of the denial plays a major role in the network of the wireless scenario by the launch pad. Here the above problem in the modeling as the threat oriented phenomena and is considered as the external aspect respectively. Here there is a huge challenge for the present designed method in which there is a lot of problem for the well accurate detection of the problems related to the protocols of thee external threat based factors and rather compared to that of the adversaries related to the internal phenomena respectively. Here in this paper a new technique is presented by the adverse implementation of the aspects related to the problems oriented attacks of the selective jamming strategy plays a crucial role in the networks of the wireless environment based scenario respectively. Here the main aspect of the system is to attack the nodes of the system in a continuous fashion followed by the continuous detection of the transmitted messages followed by the corruption in a well effective fashion where this is one of the important role in its

implementation respectively. There is a lot of analysis followed by the research based strategy takes place in the system in a well efficient manner by which related to the threat and it disturbance towards the system is a major concern apart from this study oriented performance degradation followed by the failure of the system failure plays a major role respectively. This type of the attack is mainly on the routing analogy followed by the protocol of the TCP and the routing analysis respectively. Here these types of the attacks can be easily launched by the well effective manner by the help of the classification of the packets in the real time environment followed by the relation to that of the physical layer modeling is a major concern respectively. Simulations have been conducted on the present method and a lot of analysis takes place on the large number of the data sets with respect to the different unknown environmental strategy where there is an accurate analysis takes place through the entire system in the form of the performance followed by the outcome in a well stipulated fashion respectively.

***Keywords : Classification of the packets, wireless sensor networks, service of denial, jamming selection, security aspect, data authentication, privacy control and protocol of TCP respectively***.

## 1. INTRODUCTION:

There is chance of occurrence at the place of the nodes and also at the time of the transmission of the data the dummy messages are sent which directly relate to the interference of the original signal and delay takes place finally there is damage in the system in terms of the blocking [2][3]. Apart from this it is a common problem related to the communication based on the wireless environment this can be overcome by the accurate implementation of the good security oriented data hiding technique by the name of cryptography [4][5]. But this is not applicable for all the attacks affecting the channel. But applicable to most of it [1]. So apart from this a strong method has to be designed in such a way that each and every threat has to be controlled and for effective functioning of the system [6][7]. Data transmission based on the wireless environment is a major problem and it has to be supportive from the external factors such as the attacks based on the vulnerable

phenomena respectively [10]. Here a major problem in the present increased technology is jammer based problem therefore the above mentioned technique can't give complete protection for the transmitted data.

**BLOCK DIAGRAM**

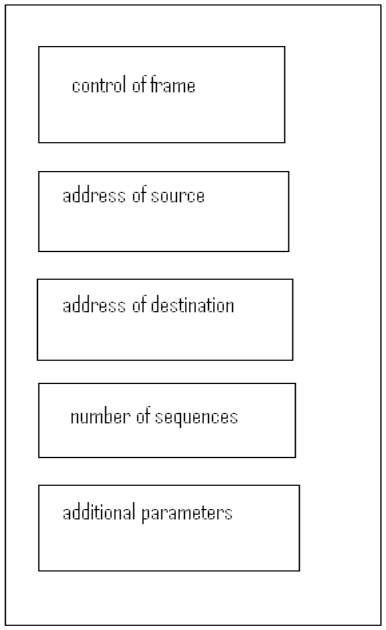


**Fig 1: Shows the block diagram of the packet classification respectively**

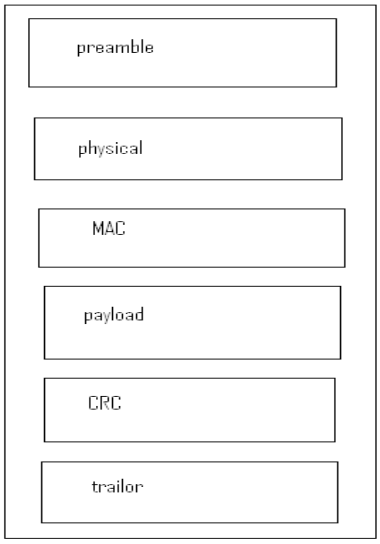


**Fig 2: Shows the generalized framework of the system respectively**

## 2. METHODOLOGY:

In this paper a method sis designed with an efficient framework where there is well effective in its implementation based aspects followed by the analysis related theme oriented scenario where there is an accurate measurement strategy takes place. Here the implementation of the present technique is shown in the below figure in the form of the block diagram which explains in a brief elaborative fashion respectively [8][9]. Here the present technique is effective and efficient in terms of the performance followed by the outcome aspects of the entire system respectively. The implementation of the present designed technique is to accurately analyze the

problems due to the several previous methods and also to study the concept related approach in a well defined fashion in which there should be an accurate control of the degraded performance followed by the implementation based strategy in a well efficient manner. Here we finally conclude that the present technique is mainly used for the improvement in the performance of the system followed by the accurate analysis related to the resultant orientation of the present technique in a well oriented approach.

## 3. EXPECTED RESULTS:

A lot of analysis have been made on the present designed technique where it is implemented with an effective framework based phenomena and also the number of the computation have been applied on the different type of the data sets efficient to that of the different environmental strategy in a well oriented aspect respectively. A comparative analysis is made between the present method to that of the several previous methods and are shown in the below figure in the form of the graphical representation. Here the present designed technique completely analyze the data and the problem oriented aspect in relative to the several previous methods in a well oriented fashion and also improve the performance of the system with respect to the well oriented analysis.

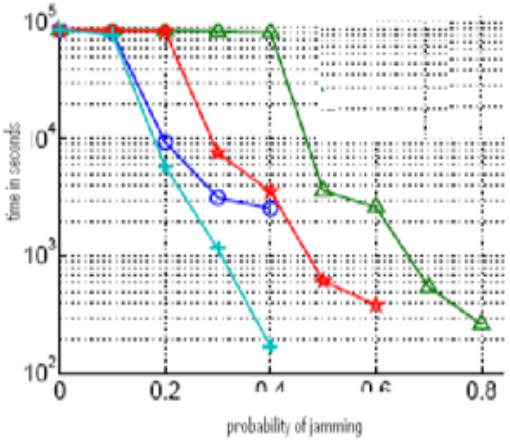


**Fig 3: Shows the graphical representation of the present method respectively**

## 4. CONCLUSION:

In this paper a method is designed with a powerful technique it is well implemented with a strategy of the efficient framework where there is an accurate analysis of the system in terms of the performance followed by the outcome of the entire system in a well oriented fashion respectively. Here the analysis is related to the networks of the wireless phenomena in which study of the attacks related to the selective jamming plays a crucial role and it

problem addressing in a well respective fashion takes place in the system respectively. Here a design oriented model takes place in the system with respect to the adversary of the internal phenomena in which attack related to the network oriented part of the jammer plays a crucial role where there is an awareness of the specification of the protocols oriented strategy related to the privacy control oriented secrets of the network sharing plays a well prominent role in its implementation aspect in a well stipulated fashion respectively. Here the transmission related to the ongoing phenomena in which initial symbol decoding takes place in the system related to the scenario of the real time environment classification of the packet transmission plays a major role towards the entire system is crucial respectively. Here the strategy followed by the routing oriented with the protocol of the TCP plays a crucial role in its implementation and these are considered as the protocol of the network in which there is a huge evaluation takes place in the system by the well stipulated attacks of the selective jamming plays a crucial role respectively. Here due to the above problem that is related to the strategy of the selective jamming phenomena in which this is a problem in which this can be easily recovered followed by the affordable loss and by the insertion of the one well equipped algorithm the problem is get solved in a well oriented fashion respectively. Here the classification of the packets with respect to the real time phenomena in which oriented with the preventing the random fashion in which there is a transformation of the jamming oriented selection plays a crucial role in its implementation aspect respectively. Here in the present analysis there is an integration of the well equipped fashion oriented with the cryptography with respect to the characteristics of the characteristics of the physical layer plays a major role and followed by the well equipped analysis takes place in the system with respect to the aspects of the privacy followed by the overhead of the communication respectively.

## REFERENCES

[1] Y. W. Law, M. Palaniswami, L. V. Hoesel, J. Doumen, P. Hartel, and P. Havinga. Energy-efficient link-layer jamming attacks against WSN MAC protocols. ACMTransactions on Sensors Networks, 5(1):1–38, 2009.

[2] L. Lazos, S. Liu, and M. Krunz. Mitigating control-channel jamming attacks in multi-channel ad hoc networks. In Proceedings of the 2nd ACM conference on wireless network security, pages 169–180, 2009.

[3] A. Chan, X. Liu, G. Noubir, and B. Thapa. Control channel jamming: Resilience and identification of traitors. In Proceedings of ISIT, 2007.

[4] T. Dempsey, G. Sahin, Y. Morton, and C. Hopper. Intelligent sensing and lassification in ad hoc networks: a case study. Aerospace and Electronic Systems Magazine, IEEE, 24(8):23–30, August 2009.

[5] Y. Desmedt. Broadcast anti-jamming systems. Computer Networks, 35(2-3):223–236, February 2001.

[6] K. Gaj and P. Chodowiec. FPGA and ASIC implementations of AES. Cryptographic Engineering, pages 235–294, 2009.

[7] O. Goldreich. Foundations of cryptography: Basic applications. Cambridge University Press, 2004.

[8] B. Greenstein, D. Mccoy, J. Pang, T. Kohno, S. Seshan, and D. Wetherall. Improving wireless privacy with an identifier-free link layer protocol. In Proceedings of MobiSys, 2008.

[9] IEEE. IEEE 802.11 standard. http://standards.ieee.org/getieee802/ download/802.11-2007.pdf, 2007.

[10] A. Juels and J. Brainard. Client puzzles: A cryptographic counte acks. In Proceedings of NDSS, pages 151–165, 1999.