IJRRECS/August 2013/Volume-1/Issue-4/259-262 **ISSN 2321-5461**

INTERNATIONAL JOURNAL OF REVIEWS ON RECENT ELECTRONICS AND COMPUTER SCIENCE

SELECTIVE JAMMING ATTACKS USING PACKET HIDING METHODS

Mettu Shailaja[1], A.Ravi Kumar[2]

[1]**M.Tech Student, Dept of CSE, Samskruti College of Engineering & Technology, Ghatkesar, R.R Dist, A.P, India**

[2]**Assistant Professor, Dept of CSE, Samskruti College of Engineering & Technology, Ghatkesar, R.R Dist, A.P, India**

ABSTRACT:

There is a lot of advancement takes place in the system by this there is a problem related aspects in the form of the threat based strategy plays a major role for the data corruption in a well respective fashion. Here this particular problem is due to the environment here is a wireless based strategy that is the transmission of the data takes place in the wireless based environment so there is a huge chance for the corruption of the data by the help of the hackers or even by the malicious attacks respectively. Now there is a huge challenge for the present method where in order to overcome the problem related to the jamming as the problem effecting the system externally is a major task. Here the accurate analysis is done by the help of the performance oriented strategy followed by the service based quality respectively. There is a huge problem related to the attacks based on the jamming oriented strategy where it is considered as one of the international technology designed in such a fashion where it is effective implemented used to compromise the system oriented network in a well effective manner followed by the complete corruption of the data in terms of the data loss or even delay in the takes place in a respective fashion. Here the threat related to the external oriented strategy is considered as the jamming effect respectively. So there is no problem with respect to the internal oriented strategy. So here the above strategy that is complete degradation of the performance takes place in the system is termed as the service oriented denial phenomena respectively. Simulations have been conducted on the present method and the accurate analysis of the system with respect to the performance based aspect followed by the accurate analysis in the entire system based outcome.

Keywords: Jammer strategy, Selective jamming, Network protocol, Design strategy, Classification of the packets, denial of service respectively.

1. INTRODUCTION

Here the present system is getting occupied by the jamming oriented strategy it is one of the malicious attacks in a considerable phenomena respectively [1]. It is termed as one of the internal threat based phenomena where many of the previous existing techniques are unable to control the attacks related to particular strategy so there is a continuous degradation of the performance takes place in the entire system respectively in a well oriented fashion [2][5]. In the wireless based strategy there is a transfer of the data in a quite reliable fashion. So here many of the users are getting attracted to this sough of the technology where in terms of the reliable transmission of their transmitted data followed by the reduced cost oriented strategy respectively. Here this is a wireless oriented scenario there is a problem in terms of the privacy based aspect respectively. So here there is a huge challenge where in order to improve the performance of the system on behalf of the proposed method where it is supposed to implement in a well effective manner in order to improve the performance of the system effectively. Here now there is a huge challenging task is to control the system from the malicious attack and some of them includes the jamming based strategy in a well effective manner respectively [3][4]. Therefore there is a huge problem with respect to this type of the attack where it continuously compromising the performance of the nodes which is involved in the present system followed by the data loss and also the corrupting of the information based on the transmitted phenomena respectively [6].

2. METHODOLOGY

In this paper a method is designed with a well effective strategy in which there is a n accurate analysis is made with respect to the improvement in the performance based strategy followed by the accurate analysis in the entire system based aspect respectively [7]. There is a huge challenge for the present method in which it is supposed to accurately analyze the problems of the several previous methods and also the respective outcome of the entire system in a quite oriented fashion respectively [8][9]. Here the implementation of the present method is shown in the below figure in the form of

the block diagram and is explained in an elaborative fashion respectively. Here we finally conclude that the present method completely overcome the problems of the several previous methods in a well efficient manner respectively [10].

BLOCK DIAGRAM

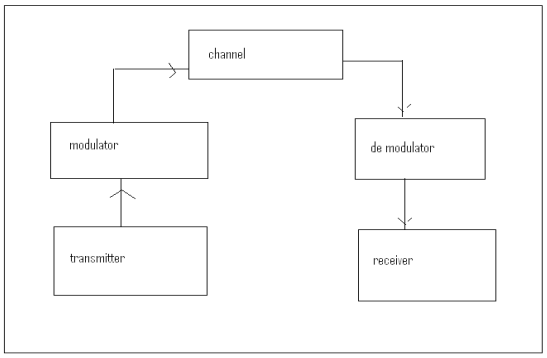

Fig 1: Shows the block diagram of the present method respectively

3. EXPECTED RESULTS

A lot of analysis is made and a number of the simulation are calculated in a very efficient manner followed by the huge computations is applied on the large number of the data sets in a well effective manner respectively. A comparative analysis is made between the present method to that of the several previous methods is shown in the below graphical representation and is illustrated in an elaborative fashion. Here the present method is effective and efficient in terms of the analysis related to the performance based strategy followed by the outcome of the entire system in a well respective fashion oriented phenomena respectively. There is a huge challenge for the present design oriented strategy in which an effective analysis is made in order to improve the performance of the system in a well effective strategy with respect to the resultant of the system.

4. CONCLUSION

In this paper a method is designed with a well effective framework for the implementation of the above successful strategy in terms of the performance based analysis followed by the accurate entire system based outcome in an entire aspect respectively. Here in the networks related to the wireless based strategy in which there is a an effective orientation of the attacks or the problems based on the jamming oriented strategy in a well efficient manner respectively. Here a model is designed based on the adversary effects of the internal strategy in a well effective manner followed by the network oriented aspect in which at the time of the attack the jammer is one part related to this particular aspect respectively. Here the theoretical analysis has to be in a perfect desired fashion followed by the specification based aspect of protocol based scenario plays a well efficient role for the accurate analysis related to the

secrets of the network sharing based aspect respectively. Here we finally conclude that the present method is well effective in terms of the implementation aspect followed by the accurate analysis in the entire system based outcome in a well respective fashion.

REFERENCES

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

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

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

[4] 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.

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

[6] A. Juels and J. Brainard. Client puzzles: A cryptographic countermeasure against connection depletion attacks. In Proceedings of NDSS,pages 151–165, 1999.

[7] 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.

[8] 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.

[9] G. Lin and G. Noubir. On link layer denial of service in data wireless LANs. Wireless Communications and Mobile Computing, 5(3):273–284, May 2004.

[10] X. Liu, G. Noubir, and R. Sundaram. Spread: Foiling smart jammers using multi-layer agility. In Proceedings of INFOCOM, pages 2536–2540, 2007.