International Journal of Advanced Information Science and Technology (IJAIST) ISSN: 2319:268
Vol.2, No.6, June 2013 DOI:10.15693/ijaist/2013.v2i6.13-16

Averting The Jamming Attacks Using Probing Technique

R.Saranyadevi [1] , D.Prabakar[2] , Dr.S.karthik[3]
[1] *II year M.E CSE, Department of Computer Science & Engineering (PG)*
SNS College of Technology, Sathy Main Road, Coimbatore-641035
[2]*Assistant professor, Department of Computer Science & Engineering*
SNS College of Technology, Sathy Main Road, Coimbatore-641035
[3]*Dean, Department of Computer Science & Engineering*
SNS College of Technology, Sathy Main Road, Coimbatore-641035

Abstract - Wireless network provides the communication only with some security threats which may have to face various difficulties. It will also lead to jamming attacks that comes under Denial Of Service (DOS) attack. Initially, the jamming attacks were mitigated by using various jammer like Constant jammer, Deceptive jammer, Random jammer, Reactive jammer. Whereas, the most preferred way of preventing those jamming attacks using probing method. It is being followed in four methods: (a) Distributed Probing scheme that transfers messages by deciding the specific path; (b) Probing Path Selection Algorithm that select solely the messages to be sent; (c) The Probing Algorithm probes each node and formulates the messages; (d) The Diagnosis Algorithm detects a node which is responsive for the subsequent node. From all these methods it is possible to resolve the attacks as from best way.

***Keywords*— Jammer, DOS, Probing Technique, Spread Spectrum, Pseudonoise**

I. INTRODUCTION

There are about two types of communication-wired and wireless. A communication is said to be in wireless if the mode of transferring of any kind of information between two are more points which are not connected at any forms. Wired communication protocol, a pair of copper wires or solid medium is required for transmission. Even though wired medium has a better transmission speed than wireless, the efficiency is best in which the signals are transferred through RF transmission among the devices and their supporting computers in a wireless communication. Some good simple known examples are Mobile, Wi-Fi, Bluetooth. In spite we may have to face many security threats due to wireless medium data transfer. Denial of Service is one of them which regret the usage of the users towards their resources. In order to reduce those problems several steps are being taken.

The data communication is interrupted unless the denial of service is eliminated. One of this process is a jamming attack (FIG 1). All the physical transmission and reception has been blocked using a jammer that prevails in the protocol and it continuously emits Radio Frequency (RF) signals that block legitimate traffic. It is possibly done by two methods. One is internal threat model that persists in the process and block a part of the network. And, the other type is an external threat model that is not a part of a network security.

There are four forms of jamming attacks. They are constant jammer, Deceptive jammer, Random jammer and Reactive jammer.

A. Constant Jammer

In this process, radio signals are emitted continuously and data are transmitted to the channel in random bits. There is no MAC layer etiquette is involved in this method. Due to constant data transfer, the channel does not become idle.

B. Deceptive Jammer

Apart from bits data transfer, series packets are transferred. Those packets deceive normal nodes. It generally checks out the preambles out of the network and remains silent.

C. Random Jammer

It chooses the jamming and sleeping processes alternatively with a specific interval of time. The time period t_j is meant for jamming and t_s is during sleeping. Both the process are not scheduled and it random.

D. Reactive Jammer

Whenever the system is idle it will stay the jammer quite. It senses the activity of jammer to set it in ON all the time and it do not consume energy.

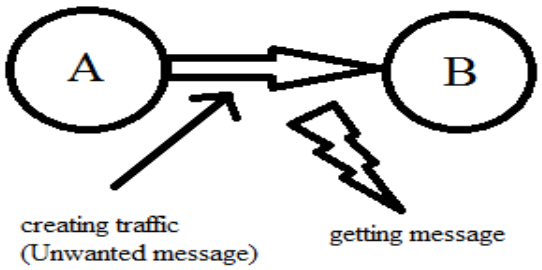

FIG 1: Jamming Attack

Anti jamming process consist of a random transmission of high-power interference signal with two steps. Initially the jammer expands the energy into jam frequency bands of interest.

Anti jamming rely on Spread Spectrum (SS) communication like spatial retreats. It has a bit level protection according to the secret pseudonoise (PN) code. It is preferred to use internal threat model instead of external threat model to protect transmission and hence the broadcasting communication is vulnerable.

II. RELATED WORKS

A. CBA

In a wireless communication standard the network requires a frequent exchange of control messages among their neighbour nodes. Irrespective of the place time and function it is being done for all channels in a network. Such messages are communicated using the control channel. Hence this might be the reason why the Denial of Service (DOS) makes it as a target function. The DOS is manifested in the form of jamming which are sophisticated for a secured network operation. Since, it is not possible for an anti jamming technique to prevent them that probably rely on spread spectrum. Cluster Based Architecture (CBA) is adopted for this with a set of clusters and each cluster has an individual control channel. Two nodes are used for this operation such as acting nodes and colluding nodes.

B. Uncoordinated Spread Spectrum (USS)

Another important profile suiting the jamming attack is that an uncoordinated spread spectrum technique. This is crucial for safe and critical operations. It is also used in several applications which always rely with integrity, availability and authenticity of the messages. A jamming based denial of service attacks such as Frequency Hopping (FH) and Direct Sequence Spread Spectrum (DSSS) is not possible to apply as the group keys are used. Overcoming all these an uncoordinated spread spectrum technique that enable anti-jamming broadcast communication without shared secrets because it has more number of receivers. They have twin ports, one is sender A that repeatedly spreads the message M using randomly selected sequences from the public sectored communication channel. The other port is B_i that tries to guess the senders choice by applying the sequences in order to dispread the message. After a certain time t_M, B_i starts dispreading and verifying M.

C. Honeypot

In WSN jamming attack takes place often which is defined as physical transmission and reception has been blocked using a jammer that prevails in the protocol. In order to mitigate the effect of jamming they have proposed a technique called honeypot in which a monitoring node is present to detect the channels used for transmission. The main concept in honeypot technique is channel switching. The entire network should coordinate in removing jamming by switching attacked channel to a new channel. It involves a transition phase in which the actual information is send through a new channel without disturbing the channel which has been attacked by the jammer. A monitoring node is responsible for channel switching. It has to decide to which channel it has to be switched and also sends a notification message along with new operating frequency for the network nodes by creating wormhole link. The jammer keeps on attacking the same channel without any knowledge of establishing a new channel.

III. PROPOSED WORK

All the resent networking protocols are not having ability to detect the jamming attacks. Due to congestion the packet dropping may not be applied in congestion control mechanisms. Link layer break is detected using link layer acknowledgements and cannot detect forward level break. TCP (Transmission Control Protocol) is a best form of giving an upper layer acknowledgement that are used to detect the end-to-end communication break. Even though it cannot have sufficient for indicating the node for communication. It is mandatory for every network connection to develop robustness for resisting the jamming attacks.

In connection with this chapter a simple and proactive distributed probing technique is implemented to detect and mitigate the jamming attacks. In his method, all the nodes of the network monitor the forwarding behaviour of other nodes proactively. For example, node B performs forwarding operation and

node A is needed to know about it, then a probe message is sent to node A which can be said as node C. Now node C is supposed to respond to probe message by sending an acknowledgement to A. when A receives response and only then the B forwards the probe message to C. The probe message is indistinguishable and so A knows that B will forward all other packets. It can detect the jamming nodes with allowed false positive rate over an environment. The delivery rate is being increased by bypassing the network communication. There are some lists of modules that are used in this protocol and they are explained in the following.

A. The Distributed Probing Scheme

In general probing techniques are used to monitor the behaviour of the mobile nodes. If we consider n nodes, there exist many chances of operations such as, having one probing node and it probes all other nodes. The other way is having k probing nodes with a space distance of r. the last way is that having n probe nodes with each spaced at infinity. The problems of nodes are being reduced if the probe messages piggyback normal packets.

B. Probing Path Selection Algorithm

There are many random paths in a routing cache that validates and produces a significant network overhead. It selects a minimum number of paths but allows for monitoring the forwarding behaviour and also has the following properties.

1. A path having the subsets on a node are eliminated.

2. The farthest node will be removed and it is to be monitored having an offer without any information.

3. The length of any path is always greater than 1.

C. Probing Algorithm

There are two ways of probing when a probe is selected. One is that from far to near node. The other is from near to far node. Choosing the probing path from far to near gives better chance since it takes only the probe message and proves goodness of all other nodes. The advantage of probing from near to far is that it generates smaller number of probing messages to detect whether it is 'good' or 'bad'.

This method has stronger way for reducing jamming attacks. When the probe node sends probe message to the far node an acknowledgement is received and all nodes show 'good'. Else it is being sent to the second farthest node. This is repeated till one node responds to the probe message. We come to know that the neighbour in the probe path is either 'DOWN' or have moved out from another location.

D. The Diagnosis Algorithm

Once the probe node detects a particular node that is responsive but the subsequent node is unresponsive which is broken at the link level or forwarding level. It searches the cache for another path until it is responsive which is formulated by two ways. One is the route through which node is responsive and the other is when it is exhausted. So, it is being broken at the forwarding level. Whenever it is unresponsive then the link is diagnosed as broken at the link layer. It is possible that both are 'BAD. Since there is no required data from the link layer break. And so, it causes false negatives. Apart from that, the node may move from the previous location to a new path and is not found by any other node.

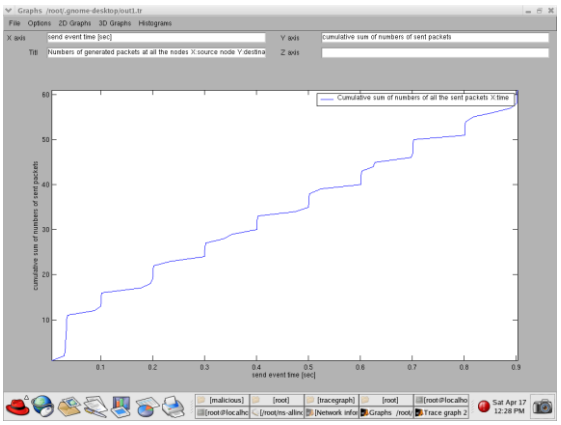

FIG.2: Comparison chart for total event time and the total packets sent.

Another possibility is that the node is moved from the network or it is 'DOWN'. Although the route discloses all the related information it seems to be expensive. So, it is detected as 'BAD', and the routing cache is updated by removing all the nodes. When the link is broken, the cache used is now truncated from all the paths. When the routing cache adds a route to the cache, it looks up the node state table and truncates them. If there is any 'BAD' node in the path, all the nodes are deleted and the process will be proceed from the next node.

This above drawn figure (FIG 2) represents the comparison of the data towards the particular packet that has been running for a time in seconds along with the

cumulative sum of numbers of the sent packets. Whenever the number of packets increases, the total duration also increases either rapidly or depending on the type of data sent. For detecting the jamming, a root node is being tested and by considering the time taken for passing the data, the malicious node is detected and in further process of calling back the nodes, it is sent through the probing techniques for averting the jamming. Thus all the nodes wherever jamming occurs is detected and averted.

IV. CONCLUSION

In this paper, the four algorithms for averting the jamming attack has been discussed and hence it is being proved that all the methods are necessary for a specific operation with their individual characteristics. The probing technique for jamming attack suit best in selecting the node of a cache information, allocating a specific channel and then move on to the main node to mitigate the attack which lead to destruction of the information.

REFERENCES

[1] X. Xiang, X. Wang and Y. Yang, "Supporting efficient and scalable multicasting over mobile adhoc networks", IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL 10, NO. 4, April 2011.

[2] Khalid A. Farhan, "Network sender multicast routing protocol:, Proceedings of seventh IEEE International conference on networking, 2008, pp.60-65.

[3] Kaan Bur, Cem Erosy, "Ad Hoc quality of service multicast routings", Computer communications, Vol. 29, 2005, pp.136-148.

[4] X. Zhang and L. Jacob, "Multicast Zone Routing Protocol in mobile Adhoc wireless networks, "Proc. Local computer networks (LCN'03), Oct.2003.

[5] Hui Cheng a, Jiannong Cao, Xingwei Wang, "A fast and efficient multicast algorithm for QOS group communications in heterogeneous network", Computer communications, Elsevier, Vol.30,2007 pp.2225-2235.

[6] I. Akyildiz, W. Lee, M. Vuran, and S. Mohanty. Next generation dynamic spectrum access cognitive radio wireless networks: A survey. Computer networks, 50(13):2127-2159, 2006.

[7] M. Cagalj, S. Capkun, and J.-P. Hubaux. Wormwhole-based anti-jamming techniques in sensor networks. IEEE Transactions on mobile computing, 6(1):100-114, 2007.

[8] V.P. Dragalin, A.G. Tartakovsky, and V.V. Veeravalli, "Multihypothesis sequential probability ratio testa,part-I: Asymptotic Optimality", IEEE Trans. Information theory, Vol.45, No. 7, pp.2448-2461, Nov.1999.

[9] Mingyan Li, Iordanis Koutsopooulos, Radha Poovendran, "Optimal jamming attack strategies and network defense policies in wireless sensor networks", IEEE transactions on mobile computing, Vol.. 9, No. 8, August 2010.

[10] G. Lin and G. Noubir. On the link layer denial of service in data wireless LANs. Wireless communication and Mobile computing, 5(3):273-284, May 2005.

[11] W. Xu . W. Trappe, Y.Zhang and T. Wood. The feasibility of launching and detecting jamming attacks in wireless networks. In Proc. of ACM MobiHoc, pages 46-57, May 2005.

[12] A. Rajeswaran and R. Negi, "DOS analysis of reservation based MAC protocols,' in proceedings of the IEEE international conference on Communications, 2005.

[13] S. Gilbert, R. Guerraoui, and C. Newport, " Of Malicious Motes and suspicious sensors", Theoretical Computer science, vol 410, no. 6-7, pp,546-569,2009.

[14] M. Tamilarasu, S. Mishra, and R. Sridhar, " Across layer approach to detect jamming attacks in wireless Adhoc networks", in proc. Of Milcom 2006, (Washington DC, USA), pp.1-7, October 2006.

[15] Yangyong Zhang Wenyuan Xu, Wade Trappe and Timothy Wood. (April 2005). The feasibility of launching and detecting jamming attacks in wireless networks. International Symposium on Mobile AdHoc Networking and Computing, pages 6-57.

[16] Y. Hu and A. Perrig, " A Survey of secure wireless Ad Hoc Networks" IEEE Comm. Magazine,vol.2, no.3,pp.28-39, May/June 2004.