International Journal of Engineering Research and Development
***e**-ISSN: 2278-067X, **p**-ISSN: 2278-800X, www.ijerd.com*
Volume 4, Issue 6 (October 2012), PP. 12-15

A Detailed Study on the Evolution of Recent Jammers in Wireless Sensor Networks

A.Mummoorthy [1], Dr.S.Suresh Kumar [2]

[1] *Research Scholar, K.S.R. College of Engineering, Tiruchengode, Namakkal Dist-637 215, TamilNadu. India.*
[2] *Principal ,Vivekanandha College of Technology for Women, Tiruchengode, Namakkal Dist-637 205, TamilNadu. India'*

Abstract:—The prospect of central control over a number of devices with the same functionality and providing the services from the repository raised the usage of networks in recent past. The practice of handling individual independent systems in a large organization did indeed posed serious difficulties over control and access of resources in a far end. The concept of organizing the individual systems into cooperative limits and the media for accessing has evolved to a greater convenience. The wireless communication era needs immediate focus on the security measures. The open structure of the wireless framework with limited protective constraints welcomes the attackers from all ends. Yet the flexibility and mobility motivates the implementation of such networks over the traditional architecture. The countermeasures predicted gives way to a new attack bypassing the new option. The well known attack in the networks is the Denial of Service attack, intended to suspend the service provided to the legitimate user. The trend used is to jam the medium by introducing noise or a distorted signal in the medium with high power transmission signals. This paper analysis the concepts of jammers and advocates the usage in affirmative means.

Keywords:—WSN, Jamming, Distributed Jamming, Denial of Service attack

I. INTRODUCTION

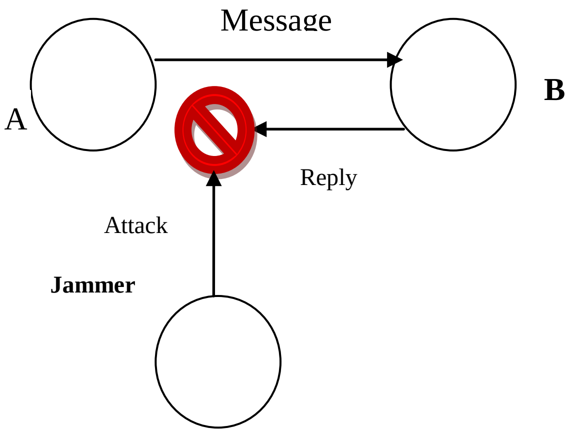
The framework of the wireless networks is to provide the services to the user irrespective of the location or the need of a physical medium. The urge of this flexibility is opted by the users on the run, to access the resources of the concern with provided authenticated identities. The need of fixation of a node in a stated place, communication links via physical cables and limitations to the capacity of the medium used, promoted the concept of deploying wireless networks. The wireless technology eliminates the difficulties of a wired network by allowing the user to access the resources with no limitations. Wireless sensor networks have a number of thousand nodes or more distributed in remote locations and all nodes are capable of requesting service simultaneously. The important factor is that not all the users are legitimate requestor of a service. There are outsiders who perform activities which disturb the security and integrity of a network. Their goal is to bother the functionality of an intended user and the services provided by the network either by blocking, distracting or by flooding the medium. The attacker acts in between two users to prevent them from communicating. The attackers learnt the ways to hide from the detection algorithms by acting as a legitimate user (spoofing) or making the network administrator to believe that there is no attack in the network.

There may be attackers internal to a network, that is, a legitimate user could also attack the network functions for his particular reasons. The wireless networks are prone to a much higher rate of attacks than the wired networks. Any attacker who gains access to a network for altering the default activities is a serious threat to the data of high confidentiality. The detection algorithms have not matched to the speed of detecting the attack in earlier stages.

This paper studies the jamming attacks of the attacker by various means and analyses the effects. The motivated study is to make sure that the jammers could be used for constructive mechanisms of conserving the security of a highly important network which cannot be compromised at any cost.

II. EXISTING TERMINOLOGIES

The jamming attacks were introduced in the military applications for transmitting the commands securely by blocking the means of eavesdropping. Then the attacks started to roam in the day to day life in radio signals, in gaming theories and to the extent in social networking. Recently a social network was blocked from its service to thousands of users. The origin of the jammers was a very simple strategy to perform the intended function. The initial jammers are categorized into four types based on their transmission of the disturbing signal.



The **constant** jammer transmits the jamming signal of high transmission power to the medium of communication regularly till the jammer is dried out of power. The constant jammer continually sends a meaningless signal just to block the network. In case of CSMA networks, prior to the transmission all the nodes would check whether the medium is free or not. The medium would never be found idle to allow the legitimate transmission. Hence the jamming attack succeeds. But considering the energy factor of the jammer, without any external power supply, it works till the battery is dried off. Once the charge is used completely, the jammer dies and the original service begins.

The **deceptive** jammer resembles the constant jammer in its activities and differs from the signal which it sends to block the intended service. This type of jammer uses the actual resource messages to be transmitted for the attack. The network users never get a chance to detect the whether the service is an attack or from the original source. The receiver would allow the transmission and the original data packets from the right source are blocked since the channel is in use. This type of jammer was introduced to evade from detection mechanisms. But the energy of the jammer is the drawback, resulting in limited time usage. The next evolution of the jammer is the **random** jammer, which was proposed with the idea of conserving the power whenever possible. The jammer is programmed to be active for a defined time and goes to sleep for a defined time. The jammer transmits a random signal such as a noise signal or any other signal for sensing the medium to be busy for a unit of time and remains idle for a period of time alternatively. This facilitates the longer lifetime of the jammer.

Eliminating the limitations of all other jammers, the **reactive** jammer is an intelligent mechanism. The jammer is activated to transmit blocking signals only when the original messages are to be exchanged. Otherwise the jammer goes to the energy conservation mode (switched off). This method is far better in conserving the power of the jammer. These types of jammer merely send a message for colliding with the original message. On collision the legitimate message is dropped.

These jammers discussed are the devices that act external to a network, on the command of attacker related or not. There are also cases in which the internal users of a particular network selfishly act to block the services of the other users. They selectively jam the networks by altering the messages of high importance such as TCP or messages of routers. These attacks are said to be **selective** jamming attacks. Instead of blocking the communication channel, the messages and their contents are altered.

III. MOTIVE OF JAMMING

The ultimate aim of jamming is to congest the communication channel with unwanted signals, never leaving a chance for the legitimate users to access the same. The channel is blocked till the waiting queue is filled and the fore coming messages are dropped. Otherwise jamming retards the complete reception of packets at the destination. The whole message could not be retrieved unless all the packets are received.

The detection algorithms work hard to identify the attack and try to prevent the possibilities. However the new attacks are capable of overcoming and eluding the algorithms to continue their mishap activities. The additional motive of a jammer is to hide from the detection algorithms and proceed with the blockage of signal.

Power management of the jammer is apart from the normal operation, but still needs certain consideration. The efficient way of using the jammer enhances the period of attack to the network. The jammers are said to have enough power as much as less than 1000 times than the legitimate transmitter to block the service. Yet energy efficient jammers are preferred and employed.

IV. DIFFERENT MODES OF JAMMING ATTACKS

Every jamming attack selects a specific area for attacking and those techniques are discussed as follows.

The jamming attacks are prominent in blocking the channel by means of a undesired signal. The CSMA networks checks for the channel to be idle and waits till the link is freed. The user finally gives up and thus the service is blocked. This jamming attack concentrates on the bandwidth and frequency of the channel. Jammers of this type are the first to be of the attack. The aim is to forward a signal equivalent or more powerful than the legitimate signal. This type originated in the broadcast of radio signals. But these attacks are easy to overcome if the frequencies are changed by the sender. Hence the need of more serious attacks raised.

The current jammers are made to block the messages that are supposed to be in place. The RTS/CTS messages constitute a pair in which either cannot be lost for a complete communication. The jammers wait for a RTS message to be transmitted and then block the other. The network waits for the reply and retransmits the message again. Till the message is blocked by the jammer, repeated transmissions occur until user identifies the reason. Similar to the blockage of RTS/CTS messages, the data packets are prevented from reaching the destination.

Jammers are also well versed with altering the authentication and claiming to be the part of the network by spoofing. Proposing reasonably allows the attacker to gain access to the services of the network. The authentication messages from new users are distracted from reaching the module for authorization. The module then disapproves any incoming request messages and thus new users are rejected.

Apart from the external attackers, the selfish users internal to the network could also jam the services and functions of the network. Being an authorized user of the network, attacker will use the medium for a considerably long time, making all other users wait for their turn to transfer the messages.

These discussions have stated the models of jamming attacks in the field today. There have been detection and prevention theories proposed to control and mitigate the jamming attacks. Countermeasures are based on the encryption of messages and securing the channel by high power transreceivers. Yet the jamming attacks are significant enough to succeed the mechanisms.

Countermeasures include the verification of the channel traffic at regular intervals, comparing with a threshold value of normal traffic and traceback methods to identify the attacker. But there are still no successive methodologies to completely eradicate the jamming attack. These countermeasures cannot be the solution to all the available attacks and newly developed immune attacks.

The following section discusses the constructive ways of using jammers in a network. The same functionalities of a jammer could be proved to be fruitful in terms of positive approach. Applications of highly important message transfer cannot compromise on the attacks. Jammers could be used for preventive measures in military and health care applications where a simple attack leads to catastrophic effects over the entire nation.

V. JAMMERS – A DIFFERENT APPROACH

Taking into consideration of the applications and efficiency measure of the sensors, they can be employed in a constructive way. The interference of signals, exclusion of noise and distorted signals needs to be removed for obtaining a good quality and security over the legitimate signals. Prevention of attacks through implementation of jammers is possible and without detection enables the source and destination to promise a reliable channel for communicating. The jammers have evolved into low power, energy efficient and are capable of high coverage regions. Jammers introduced in the military applications had the motive to prevent the adversary from eavesdropping and altering the high command to mislead the aircrafts, launch of missiles etc.

Jammers in use today are far developed than the traditional usages. Mobile applications such as cellular phones, Wireless LAN services have been disturbing one or the other. In schools and other educational institutions mobile signal jammers are employed for offering a dedicated environment for the original purpose. The holy places are too under attack by these users. The sacred activities are often disturbed by the human friendly services which enforces the implementation of the positive jammers. The selfish behaviors of some users are intolerable for the important services in civilian applications. To mitigate the jamming attacks of all kind, positive jammers are in sensible urge to be implemented.

The case of distributed jammers grouped into a network acts against all the odds. Distributed jammers are the latest development of jammers, in a size invisible to the naked eye, forming a larger boundary of coverage area and energy efficient. Understanding the importance of the war field, the communication has to be secured by all feasible means. The distributed jammer networks resemble a formation of dust, but performing the function to disrupt and suspend the attacker’s signal from every nook and corner. The dust of jammers also possesses a low self interference rate in order to avoid collision of the same motive jammers.

Although the civilian applications are simple in words the disturbances are unbearable. Considering the healthcare applications, emergency situations needs the best quality for proper analysis and recommendations of the patient in last minutes. Mostly the jammers are unaware of the location of attack which he initiates. Hence the jamming attacks need serious countermeasures at once. Denial of Service has to be provided to the attacker himself to conserve the integrity of the network applications.

VI. CONCLUSIONS

The positive and degradation effects of the jammers are analyzed after discussing the types of jammers, the models of attacks and their efficiency of today’s world. This paper supports the installation of such high efficient and reliable jammer networks to enhance the security level of the important applications and domestic usage.

REFERENCES

[1] C. Schleher, Electronic Warfare in the Information Age. Artech House,1999.

[2] R. Mallik, R. Scholtz, and G. Papavassilopoulos, “Analysis of an on-off jamming situation as a dynamic game," IEEE Trans.Commun., vol. 48,no. 8, pp. 1360-1373, Aug. 2000.

[3] D. Wood and J. A. Stankovic, “Denial of service in sensor networks,"IEEE Comput., vol. 35, no. 10, pp. 54-62, 2002.

[4] R. Negi and A. Perrig, “Jamming analysis of MAC protocols," Carnegie Mellon technical memo, 2003.

[5] J. Bellardo and S. Savage, “802.11 denial-of-service attacks: real vulnerabilities and practical solutions," in Proc. USENIX Security Symp., pp. 15-28, 2003.

[6] Wood, J. Stankovic, and S. Son. “JAM: a jammed-area mapping service for sensor networks," in Proc. IEEE Real-Time Syst. Symp., pp.286-297, 2003.

[7] G. Noubir and G. Lin, “Low-power DoS attacks in data wireless LANs and countermeasures," SIGMOBILE Mob. Comput. Commun. Rev., vol. 7, no. 3, pp. 29-30, 2003.

[8] J. M. McCune, E. Shi, A. Perrig, andM. K. Reiter, “Detection of denialof-message attacks on sensor network broadcasts," in Proc. IEEE Symp.Security Privacy, 2005.

[9] W. Xu et al., “The feasibility of launching and detecting jamming attacks in wireless networks," in Proc. ACM Int’l. Symp. Mobile Ad Hoc Netw. Comput., 2005, pp. 46-57.

[10] W. Xu, T. Wood, W. Trappe, and Y. Zhang, “Channel surfing and spatial retreats: defenses against wireless denial of service," in Proc. ACM Workshop Wireless Security, pp. 80-89, 2004.

[11] M. Li, I. Koutsopoulos, and R. Poovendran, “Optimal jamming attacks and network defense policies in wireless sensor networks," in Proc IEEE INFOCOM, May 2007.

[12] Q.Huang, H.Kobayashi, and B.Liu. “Modeling of distributed denialof service attacks in wireless networks,” in IEEE Pacific Rim Conf.Commun., Computers and Signal Process., vol. 1, pp. 113-127, 2003

[13] L.Sherriff, “Virus launches DDoS for mobile phones,” [Online]. Available:

[14] http://www.theregister.co.uk/content/l/12394.html

[15] M. Acharya and D. Thuente, “Intelligent jamming attacks, counterattacks and (counter)2 attacks in 802.11b wireless networks,” in Proc.OPNETWORK-2005 Conf., Washington DC, USA, Aug. 2005.

[16] Y.Zhang, W.Lee, and Y.-A.Huang, “Intrusion Detection Techniques for Mobile Wireless Networks,” in ACM J. Wireless Net., vol. 9, no. 5, Sept.2003, pp. 545-56.

[17] A.B.Smith, “An examination of an intrusion detection architecture for wireless ad hoc networks,” in 5th National. Colloq. Inf. Syst. Sec.Education, May 2001.

[18] O.Kachirski and R.Guha, “Intrusion detection using mobile agents inwireless ad hoc networks,” in Knowledge Media Net., Proc. IEEE Wksp.,July 10-12, 2002, pp. 153-58.

[19] W.Xu et al, “Channel surfing and spatial retreats: Defenses against wireless denial of service,” in Proc. 2004 ACM Wksp. Wireless Security,2004, pp.80-89.

[20] V. Navda, A. Bohra, S. Ganguly, and D. Rubenstein, “Using channel hopping to increase 802.11 resilience to jamming attacks,” in IEEE iNFOCOM, Mini-Conf., 2007.

[21] K. Pelechrinis, C. Koufogiannakis and S.V. Krishnamurthy, “Gamming the jammer: Is frequency hopping effective?,” in WiOpt, 2009.

[22] Sampath.A, H. Dai, H. Zheng, and B. Y. Zhao, “Multi-channel jamming attachs using cognitive radios,” in IEEE ICCCN, 2007.

[23] K. Pelechrinis, I. Broustis, S.V. Krishnamurthy and C. Gkantsidis,“ARES: An anti-jamming reinforcement system for 802.11

[24] networks,”in ACM CoNEXT, 2009.

Mr. A.Mummoorthy is presently Assistant Professor, Department of CSE, K.S.R. College of Engineering, Tiruchengode, Namakkal, Tamilnadu, India. He received the B.E from Anna University, Chennai and M.E from Anna University of Technology, Coimbatore. His research interests include Wireless Sensor Networks, Network Security. He is member of ISTE.

Prof. Dr.S. Sureshkumar is presently Principal, Vivekananda College of Technology for women, Tiruchengode. He received the B.E from National Engineering College, M.S, - Software system from Birla Institute of Technology and Science, M.Tech., from Indian Institute of Technology, Kharagpur and Ph.D., degree from Anna University, Chennai in 1988, 1993, 2000 and 2009 respectively. He has published more number of papers in refereed international journals and refereed international conferences.