Volume 2, Issue 11, November 2012 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A Comparative Assessment on the Jammers and Defensive Mechanisms in Wireless Sensor Networks

C. Silambarasan
Dept of Computer Science and Engg
K.S.R.College of Engineering,
Tiruchengode, India

M. Prakash
Asst. Prof. Dept of Computer Science and Engg
K.S.R.College of Engineering,
Tiruchengode, India

Abstract - The global applicability of the wireless technology for communication between devices has altered the entire framework for networks. Mobility of the devices yet allowed to access the services and flexibility are the stated advantages. But still the security measures need additional methodologies to prevent the illegitimate usage and attack to the legitimate users. The Denial of Service attacks (DoS), the most widespread attack to the wireless network requires great concern and resilient mechanisms. This paper discusses the motive and modes of the Denial of Service attacks and their proposed defensive mechanisms. Jammers are the devices with power efficient and easily applicable advancements to extinguish the available bandwidth of the medium. The legitimate users are blocked from their turn of service which the attacker intends. Several defense mechanisms have tried to mitigate the attacks and identify the attacking node, achieving a close success but not completely. The attackers tend to find a new mode of attack every time a defense mode is activated.

Index terms: Wireless networks, jammers, detection, DoS attack, ACK.

I. INTRODUCTION

Traditional implementations of networks required the physical location of the nodes to be stable and cables were used to connect those devices. In today's world, the necessity of wireless devices mounted and thus the services to those devices needs to be provided with the same security as the wired networks. The entry and exit points of the wired networks [12] clearly obeyed several stringent constraints. In order to obtain a service from the network, a node should be authorized by the administrator if being administered by a dedicated control station. The internet service whereas cannot limit the service and users. The densely populated internet users are raising everyday along with modes of attacks. The social networks and email service providers are the high priority zones of attacks. Places where confidential and secret messages are yet to be implemented with high secure strategies. The wireless [10] nature of the current networks has benefitted the users in many ways. Availability and access to the services without the need of static location and cables indeed simplified the structure of the networks. Users are enabled to communicate with other users or the control station through mere air medium and with proper authentication. This incremented the number of users to access and obtain services which automatically caused congestion among the legitimate users. Numerous algorithms have been proposed with different ideologies to prioritize the users and order the providence of the requested services. All of these advancements andmethodologies concentrated on the steps to enhance the efficiency of the network. But the security of the network and resources has to be ensured beyond the speed and cost of communication.

Speaking of Denial of Service attacks [9], the interesting fact is that it originated in the game theory. Players would try to participate in the ongoing game either in both ways. Every player need not be a real player of the game and thus block the service or chance of the original player. This reason does not have any serious effects over the players, but in case of the banking and financial sectors, the effects would be drastic. The network resources are made to be exhausted and unavailable for the intended users. Exhaustion of those resources is achieved by transmitting uncalled-for messages just for congesting the medium. The legitimate user is blocked or denied his/her service due to the congestion in the medium or made to wait until the packet gets discarded.

II. JAMMERS-ANALYSIS

Jammers [8] as the name suggests, originated during the war times to jam the signals of the opponent from sending unwanted signals with inappropriate messages to distract the people. Counter measures were carried out by transmitting a high frequency signal into the medium to exhaust the attacker's signal. The low power signal would be overlapped such that it would be lost and cannot be received by the intended device.

A transmitter (antenna) is made to send a signal of an encrypted message towards a destination where another antenna (receiver) would collect the signal. The transmitted signal uses a particular frequency band and strength to reach the destination. Jammer would act to disrupt the signal by forwarding the **attack signal**[1]of the same frequency but of high power to override the same. However these jammers are used for blocking the attack signal which now has evolved to be a serious device for Denial of Service (DoS) attack.Detection of the attack signal is obvious for tackling the attack. The

jammers impose the attack in two modes; in the former the attack signal could be easilyspotted. The signal would be a distorted noise or a scrambled messageof disturbance. The latter attack has been modified to evade detection and identification from the other end. The receiver would not doubt the activity since the network would be absolutely normal. The ultimate aim would be to block the original signal from reaching the correct destination.

A. Analysis on the types of Jammers

The jammers may be of mechanical or electronic types. Mechanical jammers are implemented to reflect the signal when focused at a particular direction. They are physical type of jammers. These jammers are not capable of selective attack on any specific frequencies but pose a serious attack on the signals. On the other hand, the electronically activated jammers perform on the determined frequencies. These devices are energy efficient [4], low power and sincere jamming technological advancements. Radio jammers [2] are considered to be the most probable jammers to be used in networks.

The motive of the jammers is to transmit unwanted noise [14], distorted music, scrambled voice, unclear messages, high frequency signals into the network for exhausting and wasting the dedicated medium. The nodes since programmed to wait if the medium is sensed to be busy, continue to wait until the packet is expired. Considering internal the network, the jammers act to stop the transmitted packets from the legitimate users which are comparatively tougher than blocking a signal. Individual packets are prevented from reaching their intended receiver by various means such as flooding the medium with meaningless packets. The final output is to deny the service to the requesting user by keeping the medium busy for a long time making the user to give up the idea of transmission.

On the whole the jammers are of five types based on the time of their activity and mode of attacks.

1. Continuous Jammers
2. Impersonate Jammers
3. Unsystematic Jammers
4. Systematic Jammers
5. Exacting Jammers

The **continuousjammers** [6][11][13] transmit the jamming or attack signal into the medium at a constant rate. Since the jamming signal uses the medium, the other users will not sense the medium to be free for their legitimate service. The packets transmitted by these jammers are random meaningless messages. The jammers are small electronic devices powered by a battery with limited power resources. Hence after a considerable time, the jammer dries its battery and thus the medium is retrieved from the attack. Even an energy efficient jammer could not last for a considerable time but still for a limited span the jammer completely blocks the services in a network. The packets could be identified from the content it holds and thus the attacker. The route could be blocked to prevent the network from attack.

The attack packets can lead to the jammer node if the packets are analyzed and found to be malicious. This problem was overcome by altering the contents of the message packets sent by the jammer.

Impersonate jammers [11][13] sends the packets which resemble the original packets. The network administrator would not try to suspect the packets and thus allows the packets into the network. Yet these jammers are not energy efficient and dry out soon after. The only advantage is that it evades the detection mechanisms for a longer period.

Unsystematic jammers [25][11][13] are the foundation of energy efficient jammers. These jammers extended their life span by limiting the time of activity. Packets are sent from these jammers at a random time rather than continuously thus serving for a longer time. The jammers would alternate their activity time that is they would be on for certain period of time and switched on for a certain time. Conserving the power at regular intervals increased their lifetime, causing a threat to the network.

Systematic jammers[11] [13] are the intelligent jammers of all other types. Unlike the unsystematic jammers, they follow a strict order to be switched on and off. These are highly energy efficient and the most significant in attacking the resources. This type of jammers waits for the sender and receiver nodes to start the communication process and then gets activated. The mode of attack is simplified and the attack becomes more vulnerable to the network. If there is no communication between the nodes, then the jammers remains idle, conserving the energy. Moreover the packets sent over the medium are similar to the legitimate data packets raising no different pattern to awaken the defense mechanisms. The performance of the network is greatly affected till the jammer is isolated and relieved from its normal function where the detection of these jammers involve more computations, time and proper analysis. Since these jammers do not introduce any serious changes in the patterns of the packets, detection algorithms require more knowledge over the identification process. The jamming node can act internal to the network or can be a compromised [5] user. In such cases the jammer is aware on the details and contents of the data and control packets [3] being transferred between the nodes. Adversary node can be hidden from the attacking pattern and can evade the detection algorithms completely.

Exacting jammers are considered to be the critical jammers which have to be spotted immediately before irrecoverable changes occur in the networks. The exacting jammers determine the nature of the data packet sent in between the nodes of a network. Unless those packets are of high importance [14], they are free to move. Packets such as route request [7] or route response [7] or a packet of either important data or control flow would readily be subjected to jamming attack. The source of jamming attack, being a part of the original network, defines the longer time for suspicion.

B. Destination of the Jamming Attacks

The attack of a jammer may be implied on any of the following packets. The CTS/RTS messages are the requests made and permit messages for a packet to initiate a communication process between the sender and receiver nodes. The

node wishing to transmit a packet forwards a Request To Send (RTS) message and waits for approval. Once Clear To Send (CTS) message is obtained, the transmission begins (The CTS message quiets all wireless stations in its area to avoid crash and enables the sender of the RTS message to begin data transfer). The jammer may jam the transmission of these message packets causing incomplete communication between the medium and the network. Without the response message (CTS) the transmission cannot occur. Similarly without a request message (RTS) there would be no clear message. The next mode of attack occurs in the Acknowledgement messages (ACK). The message is broken into a number of smaller packets for easier transmission. For every packet received there should be an acknowledgement message. Otherwise the sender thinks that the packet is lost and retransmits the previous packet. If the ACK are jammed, the communication process repeatedly retransmits until the ACK is received.

Likewise the contents of the messages can be altered. The contents of the message may bet the data or the destination address or even the route it selects. The changes in the route information and the destination would cause the packets to be misled and get lost in the widespread wireless network. The altered address of the packet would affect the confidentiality of the packet in sectors of military and financial applications. The altered data of the messages would cause adverse effects in medical applications.

The common jammer would simply jam the frequency used for the communication process. Irrespective of the type of packets and the contents they hold within, the band can be easily jammed without any analyses on the packets. The jamming of the frequency would cause the communicating nodes to wait until the medium is free. Unaware of the attack under process, the legitimate nodes wait for an infinite time or until the administrator finds out the attacker.

III. DEFENSIVE MECHANISMS

The proposed mechanisms have been trying to mitigate, to prevent the network under attack. The detection involves monitoring the network and note down the changes from the normal functioning. The network administrator would keep track of the events occurring in the network at all conditions and time spans. Differences from the observed normal values would help to detect the attack in the network. With the obtained abnormal values, the attacker could be traced back and the activities could be blocked from further damage to the resources of the network.

The functioning of the network at normal time, at peak time and during the attack could be comparatively analyzed with the help of default metrics called threshold values. The metrics would be the traffic flow in the medium, the signal usage and the number of packets being transmitted in every route of the network. These values are estimated and maintained by the network administrator. Then the same estimations are calculated periodically and compared to the predetermined values of the administrator. The consistency value of the network is the measurement of the packet flow at times of congestion in a medium. These comparisons are clearly made to avoid the feasibilities of false positives and false negatives. Signature based analysis involved the maintenance of a unique identity for the packets to be sent from the same sender. The same concept could be used for analysis of the attack packets. The attack packets may possess a same pattern in which they originate from the same node or consist of the same route information. Based on these similar patterns, the attack could be mitigated. Possession of the same pattern may be legitimate in some cases; hence serious analysis has to be made to confirm the attack in a network.

Encryption is the process of converting messages or information in such a way that adversary or hackers cannot read it. In an encryption scheme, the message or information isencoded using an encryption algorithm, turning it into an unreadable cipher text.Encrypted messages are not the complete solution forjamming attack since a jammer does not need to know the message but it just blocks the path of the packet. A compromised node could know the algorithms and keys selected for the encryption and decryption. It may be a solution for the jammers which try to alter the data, path entered into the packet header but not for radio jammers. Cooperation among the nodes in a network is needed for the analysis and cross verification of the consistency and confidentiality of the messages sent. In a condition where the nodes are jammed from sending the analyzed values to other nodes for verification, the attack could not be detected and diagnosed. Understanding the fact that the presence of a jammer needs to be confirmed at a faster rate and with low false positive rate ensures the security of the network, detection and preventive mechanisms have to be stronger.

The layer of the attack should be determined initially, followed by the retrieval of adequate information on the source of attack and ultimately the measures taken to trace the path to find the source needs in depth knowledge on the participating nodes and the details on the routers. Complete knowledge sectors the mode of attack and the optimal solution for the recovery of the attacked data and other resources.

IV. CONCLUSION

This paper discusses the activities of the jammers and the possible countermeasures present today. Yet the solution to mitigate and prevent the evolving attacks needs to be framed. Yielding the solution for the jammers is the definite way to ensure secure transmission of data to and fro in the limitless wireless networks.

REFERENCES

[1] T. X. Brown, J. E. James, and A. Sethi. "Jamming and sensing ofencrypted wireless ad hoc networks". In *Proceedings of MobiHoc*, pages120–130, 2006.

[2] M. Cagalj, S. Capkun, and J.-P. Hubaux. "Wormhole-based antijammingtechniques in sensor networks". *IEEE Transactions on MobileComputing*, 6(1):100–114, 2007.

[3] A. Chan, X. Liu, G. Noubir, and B. Thapa. "Control channel jamming:Resilience and identification of

traitors". In*Proceedings of ISIT*, 2007.

[4] Y. W. Law, M. Palaniswami, L. V. Hoesel, J. Doumen, P.HartelandP. Havinga. "Energy-efficient link-layer jamming attacks against WSNMACProtocols".ACMTransactions *on Sensors Networks*, 5(1):1–38, 2009.

[5] L. Lazos, S. Liu, and M. Krunz. "Mitigating control-ChannelJammingattacks in multi-channel ad hoc Networks". In *Proceedings of the 2nd ACM conferenceon wirelessnetwork security*, pages 169–180, 2009.

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

[7] X. Liu, G. Noubir, and R. Sundaram."Spread: Foiling SmartJammersusing multi-layer agility". In*Proceedings of INFOCOM*, pages2536–2540, 2007.

[8] M. Strasser, C. Popper, and S. Capkun. "Efficient uncoordinated fhssanti-jamming communication". In *Proceedings of MobiHoc*, pages 207–218, 2009.

[9] M. Strasser, C. Popper, S. Capkun, and M. Cagalj. "Jamming-resistantkey establishment using uncoordinated frequency hopping". In *Proceedings of IEEE Symposium on Security and Privacy*, 2008.

[10] ThuenteandM. Acharya. "Intelligent jamming in wireless networkswith applications to 802.11 b and other networks". In *Proceedings ofthe IEEE Military Communications Conference MILCOM*, 2006.

[11] M. Wilhelm, I. Martinovic, J. Schmitt, and V. Lenders. "Reactivejamming in wireless networks: How realisticis the threat?" In*Proceedings of WiSec*, 2011.

[12] W. Xu, W. Trappe, Y. Zhang, and T.Wood. "The feasibility of launchingand detecting jamming attacks in wireless networks". In *ProceedingsofMobiHoc*, pages 46–57, 2005.

[13] W. Xu, T.Wood, W. Trappe, and Y. Zhang. "Channel surfing and spatial retreats: defenses against wireless denial of service". In Proceedings ofthe 3rd ACM workshop on Wireless security, pages 80–89, 2004.

[14] Alejandro Proano and Loukas Lazos. "Packet-Hiding Methods for Preventing Selective Jamming Attacks". IEEE Transactions on dependable and secure computing, Vol. 9, No. 1, January/February 2012.

