National Conference on Advances in Computer Science and Applications with International Journal of Computer Applications (NCACSA 2012)
Proceedings published in International Journal of Computer Applications® (IJCA)

Defense against Dos Attack using Monitoring Node

Ann Mary Varghese
II[nd] year ME C&C
IT Department
PSNACET
Dindigul

K. Selvaraj
Associate Professor
IT Department
PSNACET
Dindigul

ABSTRACT
Consider a scenario where a sophisticated jammer jams an area in which a single-channel random access based wireless sensor network operates. The jammer controls the probability of jamming and the transmission range in order to cause maximal damage to the network in terms of corrupted communication links. The jammer action ceases when it is detected by the network and a notification message is transferred out of the jammed region. In this paper introduce a network defense policy node for monitoring the jammer in order to overcome from attack to network. The monitoring node misleads the jammer that the server is down but actually the server is not down. This paper provides valuable insights about the structure of the jamming problem and associated defense mechanisms for achieving desirable performance.

Keywords
Jamming, wireless sensor network, network defense policy node, security, optimization.

1. INTRODUCTION
The fundamental characteristic of wireless networks that renders them more vulnerable to attacks than their wire line counterparts is the open, shared nature of their medium. This exposes them to two fundamentally different attacks: passive and active attacks. In the former ones, the malicious entity does not take any action apart from passively observing the ongoing communication that is, eavesdropping with the intention to intervene with the privacy of network entities involved in the transaction. On the other hand, in active attacks the attacker is involved in transmission as well. Depending on attacker objectives, different terminology is used. If the attacker abuses a protocol with the primary goal to obtain performance benefits itself, the attack is referred to as misbehavior. If the attacker does not directly manipulate protocol parameters but exploits protocol semantics and aims at indirect benefits by unconditionally disrupting network operation, the attack is termed jamming or Denial-of-Service (DoS). Jamming can disrupt wireless transmission and occur either unintentionally in the form of interference, noise or collision at the receiver.

A wireless sensor network (WSN) consists of spatially distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, motion or pollutants and to cooperatively pass their data through the network to a main location. The more modern networks are bi-directional, also enabling control of sensor activity. The development of wireless sensor networks was motivated by military applications such as battlefield surveillance; today such networks are used in many industrial and consumer applications, such as industrial process monitoring and control, machine health monitoring, and so on. The WSN is built of "nodes" where each node is connected to one sensor. Each such sensor network node has typically several parts: a radio transceiver with an internal antenna or connection to an external antenna, a microcontroller, an electronic circuit for interfacing with the sensors and an energy source, usually a battery or an embedded form of energy harvesting. Size constraints on sensor nodes result in corresponding constraints on resources such as energy, memory, computational speed and
communications bandwidth. The topology of the WSNs can vary from a simple star network to an advanced multi-hop wireless mesh network. The propagation technique between the hops of the network can be routing or flooding.

2. OVER VIEW OF JAMMING
The most trivial way of disrupting a wireless network is by generating a continuous high power noise across the entire bandwidth near the transmitting and/or receiving nodes. The device that generates such a noise is called a jammer and the process is called jamming. Jammers, which jam the network with the knowledge of the protocol, are termed as protocol aware jammers. Jamming and its countermeasures have a long history in military applications.

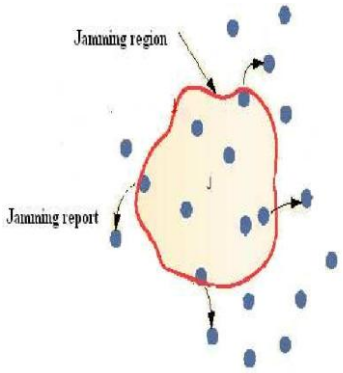

Figure 1.1 Jammed Region Report the Attack to their Neighbor

3. SECURITY FOR SENSOR NETWORK
Network defense includes actions taken via computer networks to protect, monitor, analyze, detect and respond to network attacks, intrusions, disruptions or other unauthorized actions that would compromise or cripple defense information systems and networks. As the sensor networks can also operate in an ad hoc manner the security goals cover both those of the traditional networks and goals suited to the unique constraints of ad hoc sensor networks.

The security goals are classified as primary and secondary. The primary goals are known as standard security goals such as Confidentiality, Integrity, Authentication and Availability (CIAA). The secondary goals are Data Freshness, Self-Organization, Time Synchronization and Secure Localization. The primary goal such as Data Confidentiality is the ability to conceal messages from a passive attacker so that any message communicated via the sensor network remains confidential. This is the most important issue in network security. A sensor node should not reveal its data to the neighbors. Data Authentication ensures the reliability of the message by identifying its origin. Attacks in sensor networks do not just involve the alteration of packets; adversaries can also inject additional false packets. Data authentication verifies the identity of the senders and receivers. Data authentication is achieved through symmetric or asymmetric mechanisms where sending and receiving nodes share secret keys. Due to the wireless nature of the media and the unattended nature of sensor networks, it is extremely challenging to ensure authentication. Data integrity in sensor networks is needed to ensure the reliability of the data and refers to the ability to confirm that a message has not been tampered with, altered or changed. Even if the network has confidentiality measures, there is still a possibility that the data integrity has been compromised by alterations. The integrity of the network will be in trouble when: (1) A malicious node present in the network injects false data. (2) Unstable conditions due to wireless channel cause damage or loss of data. Data Availability determines whether a node has the ability to use the resources and whether the network is available for the messages to communicate. However, failure of the base station or cluster leader's availability will eventually threaten the entire sensor network. Thus availability is of primary importance for maintaining an operational network.

The secondary goals are as follows:-Data Freshness- Even if confidentiality and data integrity are assured, there is a need to ensure the freshness of each message. Informally, data freshness suggests that the data is recent, and it ensures that no old messages have been replayed. To solve this problem a nonce, or another time-related counter, can be added into the packet to ensure data freshness. Self-Organization in which wireless sensor network is a typically an ad hoc network, which requires every sensor node be independent and flexible enough to be self-organizing and self-healing according to different situations. There is no fixed infrastructure available for the purpose of network management in a sensor network. This inherent feature brings a great challenge to wireless sensor network security. If self-organization is lacking in a sensor network, the damage resulting from an attack or even the risky environment may be devastating. Time Synchronization in which sensor network applications rely on some form of time synchronization. Furthermore, sensors may wish to compute the end-to-end delay of a packet as it travels between two pair wise sensors. A more collaborative sensor network may require group synchronization for tracking applications. Secure Localization is the utility of a sensor network will rely on its ability to accurately and automatically locate each sensor in the network. A sensor network designed to locate faults will need accurate location information in order to pinpoint the location of a fault. Unfortunately, an attacker can easily manipulate no secured location information by reporting false signal strengths, replaying signals.

4. REVIEW ON PREVIOUS WORK ON JAMMING ATTACK

The following are some of the reviews of the jamming attacks. According to the A.D. Wood and J.A. Stankovic, (2002) had investigated on unless the developers take security into account at design time, sensor networks and the protocols they depend on will remain vulnerable to denial-of-service attacks. DoS attacks again sensor networks may permit real-world damage to the health and safety of people. The limited ability of individual sensor nodes to thwart failure or attack makes ensuring network availability more difficult. Developers build sensor networks to collect and analyze low-level data from an environment of interest. Sensor networks may be deployed in a host of different environments. In this project provide taxonomy of DoS attacks launched against sensor networks from the physical up to the transport layer. But the disadvantage of this project it does not consider security.

On link layer DoS in data WLAN by G. Lin proposed that LDPC(Low Density Parity Check) code is introduced as to defend against low energy attacks. But the disadvantage of this paper is aggressive attacks are not considered.

M. Li, I. Koutsopoulos and R. Poovendran (2010) had investigated on Denial of Service (DOS) attack is generally defined as a network-based attack that disables one or more resources, such as a wireless Sensor network router or server. These attacks may crash servers, tie up services or consume all available wireless network bandwidth, sometimes hampering a network for days to months. DOS attacks range in complexity. They present the design and implementation of Kill- jammer attacks, a kernel extension to protect Wireless servers against DDOS attacks that masquerade as _ash crowds. Kill-jammer provides authentication using graphical tests but is different from other systems that use graphical tests. They include in the formulation the attack detection and the transfer of the attack notification message out of the jammed area. They capture the impact of available knowledge of the attacker and the network about the other's strategies. For the case of partial knowledge, the attacker and the network optimize with respect to the worst-case or the average-case strategy of the other. They extend the basic model to the case of multiple monitoring nodes and controllable jamming transmission range and suggest a simple efficient jamming strategy**.**

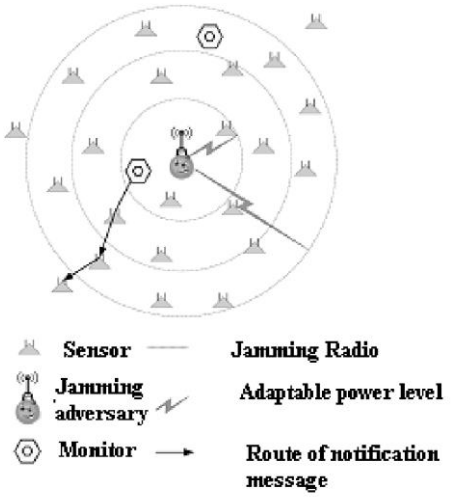

Figure 1.2. Illustration of jamming attack

Y.W. Law, L. van Hoesel, J. Doumen, P. Hartel, and P. Havinga (2009) had investigated on a typical wireless sensor node has little protection against radio jamming. The situation becomes worse if energy-efficient jamming can be achieved by exploiting knowledge of the data link layer. Encrypting the packets may help to prevent the jammer from taking actions based on the content of the packets, but the temporal arrangement of the packets induced by the nature of the protocol might unravel patterns that the jammer can take advantage of, even when the packets are encrypted. By looking at the packet interarrival times in three representative MAC protocols, S-MAC, L-MAC and B-MAC, we derive several jamming attacks that allow the jammer to jam S-MAC, L-MAC and B-MAC energy efficiently. But this protocol has certain disadvantage. There is a clustering in the S-MAC. S-MAC are based on clustering a countermeasure would naturally be to prevent clustering based analysis from being feasible. The disadvantage of L-MAC is to increase the difficulty in estimating the slot size. Also the negative impact on the bandwidth of the protocol.

M. Cagalj, S. Capkun, and J.-P. Hubaux (2007) had investigated on due to the nature, wireless sensor networks are perhaps the most vulnerable

category of wireless networks to “radio channel jamming”-based Denial-of-Service (DoS) attacks. An adversary can mask the events that the sensor network should detect by stealthily jamming an appropriate subset of the nodes; in this way, they prevent them to report what they are sensing to the network operator. Therefore, in spite of the fact that an event is sensed by one or several nodes (and the sensor network is fully connected), the network operator cannot be informed on time. They show how the sensor nodes can exploit channel diversity in order to establish wormholes out of the jammed region, through which an alarm can be transmitted to the network operator. They propose three solutions: the first is based on wired pairs of sensors; the second relies on frequency hopping, whereas the third is based on a novel concept called uncoordinated channel hopping. They develop appropriate mathematical models to study the proposed solutions. In this project, they investigate an attack where the attacker masks the event (event masking) that the sensor network should detect by stealthily jamming an appropriate subset of the nodes. In this way, the attacker prevents the nodes to report what they are sensing to the network operator. Timely detection of such stealth attacks is particularly important in scenarios in which sensors use reactive schemes to communicate events to the network sink. The solution to this problem is far from trivial: proactive schemes, in which sensors spend their time (and battery) assessing the state of their communication links are clearly suboptimal; equally, jamming detection schemes are generally over-sensitive and generate many false alarms making the system vulnerable to straight-forward Denial of Service (DoS) attacks. The disadvantage of this project is system frequently triggers an alert when there is no intrusion (false alarm), then either system managers will begin to ignore the alarms, or much time will be wasted analyzing the false alarms. The attacker can potentially learn (by scanning the available channels) that there is some activity on the channels occupied by transmitters. In this way, the attacker can avoid loosing time on jamming currently unused channels.

W. Xu, T. Wood, W. Trappe, and Y. Zhang, (2007) had investigated on wireless sensor networks are susceptible to interference that can disrupt sensor communication. In order to cope with this disruption, explore channel surfing, whereby the sensor nodes adapt their channel assignments to restore network connectivity in the presence of interference. This project explore two diff erent approaches to channel surfing: coordinated channel switching, where the entire sensor network adjusts its channel; and spectral multiplexing, where nodes in a jammed region switch

channels while nodes on the boundary of a jammed region act as radio relays between diff erent spectral zones. For spectral multiplexing, they have devised both synchronous and asynchronous strategies to facilitate the spectral scheduling needed to improve network fidelity when sensor nodes operate on multiple channels. In designing these algorithms, they have taken a system-oriented approach that has focused on exploring actual implementation issues under realistic network settings. They have implemented the experimental results show that these strategies can each repair network connectivity in the presence of interference without introducing significant overhead. As wireless networks become increasingly pervasive, it is very likely that the radio environment will not be favorable. In channel surfing, those nodes that detect themselves as jammed nodes should immediately switch to another orthogonal channel and wait for opportunities to reconnect to the rest of the network. After the jammed nodes lose connectivity, their neighbors, which we refer to as boundary nodes, will discover the disappearance of their jammed neighbor nodes and temporally switch to the new channel to search for them. If the lost neighbors are found on the new channel, the boundary nodes will participate in rebuilding the connectivity of the entire network. The two schemes used this project is coordinated channel switching and spectral multiplexing. The major challenge facing in the coordinated channel switching is the fact that unreliable

links can cause some nodes to miss a channel switch notice. For spectral multiplexing, the primary challenge lies in the fact that the boundary nodes must carefully decide when they should be on which channel so that they can minimize the number of packets not delivered due to the sender receiver frequency mismatch.

5. PROPOSED METHOD

With existing literature the project can contribute the proposed as derive the optimal attack and optimal defense strategies as solutions to optimization problems that are faced by the attacker and the network, respectively, by including in the formulation energy limitations. For attack detection, this project provides a methodology and an optimal detection test that derives decisions based on the percentage of incurred collisions compared to the nominal one. The project includes in the formulation the attack detection and the transfer of the attack notification message out of the jammed area. It captures the impact of available knowledge of the attacker and the network about the other's strategies. For the case of partial knowledge, the attacker and the network optimize with respect to the worst-case or the average-case strategy of the other. This project extends the basic model to the case of multiple monitoring nodes and controllable jamming transmission range and suggests a simple efficient jamming strategy.

In my paper provides valuable insight about the structure of the jamming problem and associated defense mechanisms using the wireless sensor node implementation and network defense policy node implementation. In wireless sensor node implementation we create a wireless sensor node to communicate with their neighbor nodes and share the data via wireless network. In network defense policy node implementation making network policy node to communicate with sensor node. The network defense policy node monitoring the jammer when it is attacked to the network. When the jammer send the message to the server in order to attack the network the monitoring node consist of proxy. When the jammer send multiple message to the server the proxy identify whether it is a jammer or a client by setting a threshold value. At that time the proxy send duplicate message to the jammer. Again the jammer send the multiple message the proxy send a message that the server is down by misleading the jammer. But actually the server is working properly.

6. CONCLUSION

This project provides valuable insight about the structure of the jamming problem and associated defense mechanisms using the wireless sensor node implementation and network defense policy node implementation. In wireless sensor node implementation we create a wireless sensor node to communicate with their neighbor nodes and share the data via wireless network. In network defense policy node implementation making network policy node to communicate with sensor node.

7. REFERENCES

[1] 1.A. D. Wood and J. A. Stankovic (2002), "Denial of Service in Sensor Networks," Computer, vol. 35, no. 10, pp.54-62.

[2] 2..A. M. Mathai (1999), "An Introduction to Geometrical Probability", Gordan and Breach Science Publishers.

[3] C. D. M. Cordeiro and D. P. Agrawal (2006),"Ad Hoc and Sensor Networks Theory and Applications. World Scientific.

[4] C. W. Helstrom(1995), Elements of Signal Detection and Estimation. Prentice-Hall.

[5] 5.D. P. Bertsekas and R. G. Gallager(1992), Data Networks, second ed. Prentice Hall.

[6] 6.G. Lin and G. Noubir, (2005)" On Link-Layer Denial of Service in Data Wireless LANs," Wiley J. Wireless Comm. And Mobile Computing, vol. 5 no. 3, pp 273-284.

[7] 7 .J. Jung, V. Paxson, A. W. Berger, and H. Balakrishnan(2004), "Fast Portscan Detection Using Sequential Hypothesis Testing," Proc. IEEE Symp. Security and Privacy.

[8] 8..J. M. McCune, E Shi, A. Perrig, and M. K. Reiter(2005), " Detection of Denial-of-Message Attacks on Sensor Networks Broadcasts," Proc. IEEE Symp. Security and Privacy.

[9] 9.M. Cagalj, S. Capkun, and J.-P. Hubaux(2007), "Wormhole-Based Anti-Jamming Techniques in Sensor Networks," IEEE Trans. Mobile Computing, vol. 6, no. 1, pp 1-15.

[10] 10.M. Li, I. Koutsopoulos, and R. Poovendran(2007), " Optimal Jamming Attacks and Defense Policies in Wireless Sensor Networks," Proc. IEEE INFOCOM,.

[11] 11.M. Raya, J.-P Hubaux, and I. Aad(2004), "DOMINO: A System to Detect Greedy Behavior in IEEE 802.11 Hotspots," Proc. Second Int'l Conf. Mobile Systems, Applications and Services (MobiSys '04).

[12] 12.P. Kyasanur and N. Vaidya(2005), "Selfish MAC Layer Misbehavior in Wireless Networks," IEEE Trans. Mobile Computing, vol. 4, no. 5, pp. 502-516.

[13] 13.R. Mallik, R. Scholtz, and G. Papavassilopoulos(2000), "Analysis of an On-Off Jamming Situation as a Dynamic Game," IEEE Trans. Comm., vol. 48, no. 8, pp. 1360-1373.

[14] 14.R. Negi and A. Perrig(2003), "Jamming Analysis of MAC Protocols," Carnegie Mellon Technical Memo,.

[15] 15.S. Radosavac, I. Koutsopoulos, and J. S. Baras(2005), "A Framework for MAC Protocol Misbehavior Detection in Wireless Networks," Proc. ACM Workshop Wireless Security (Wise).

[16] 16.V. Coskun, E. Cayirci, A. Levi, and S. Sancak(2006), "Quarantine Region Scheme to Mitigate Spam Attacks in Wireless Sensor Networks," IEEE Trans. Mobile Computing, vol. 5, no. 8, pp. 1074-1086.

[17] 17.V. P. Dragalin, A.G. Tartakovsky(1999), and V. V. Veeravalli, "Multihypothesis Sequential Probability Ratio Tests- Part 1: Asymptotic Optimality," IEEE Trans. Information Theory, vol. 45, no. 7, pp. 2448-2461.

[18] 18.W. Xu, T. Wood, W. Trappe, and Y.Zhang(2007), "Channel Surfing: Defending Wireless Sensor

Networks from Interference," Proc. IEEE Int'l Conf. Informtion Processing in Sensor Networks (IPSN),.

[19] 19.W. Xu, W. Trappe, Y. Zhang, and T. Wood(2005), " The Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks," Proc. ACM MobiHOC,.

[20] 20.Y. W. Law, L. van Hoesel, J. Doumen, P. Hartel, and P. Havinga(2009), "Energy Efficient Link-Layer Jamming Attack Against Wireless Sensor Networks MAC Protocols," ACM Trans. Sensor Networks, vol. 5, no. 1, pp. 1-38.