ISSN 2395-695X (Print)
ISSN 2395-695X (Online)
Available online at www.ijarbest.com

International Journal of Advanced Research in Biology Ecology Science and Technology (IJARBEST)
Vol. I, Special Issue I, August 2015 in association with VEL TECH HIGH TECH DR. RANGARAJAN DR. SAKUNTHALA ENGINEERING COLLEGE, CHENNAI
National Conference on Recent Technologies for Sustainable Development 2015 [RECHZIG'15] - 28th August 2015

Mitigate Jammer Disrupt In Wireless Sensor Networks Using Elliptical Curve Cryptosystem

S.Sageengrana[#1], K.Vengateshan[#2], G.Ganeshkumar[#3],A S Vijay[#4]
[#1]Assistant professor,[#2,#3,#4] UG Scholar Students
Department of Computer Science and Engineering
[#1,#2,#3,#4]*Vel Tech High Tech Dr.Rangarajan Dr.Sakunthala Engineering College ,Chennai-600 062,*

ABSTRACT:

Accurately determining locations of nodes in mobile wireless network is crucial for a myriad of applications. Unfortunately, most localization techniques are vulnerable to jamming attacks where the adversary attempts to disrupt communication between legitimate nodes in the network. In this paper, we propose an approach to localize a wireless node by using jamming attack as the advantage of the network. Our localization technique is divided into two steps. The indirect measurement scheme used is, "Received Signal Strength"(RSS) which is used to locate the position of the jammer but not with accuracy. The direct measurement scheme is used to locate the accurate position of the jammer using "Jamming Signal Strength"(JSS) but does not provide accurate security. Hence to overcome this problem, "Elliptical Curve Cryptosystem(ECC) model is used to provide security of data. Accurate and low-cost sensor localization is a critical requirement for the deployment of wireless sensor networks in a wide variety of applications. Hence Indirect scheme and Direct scheme are used to localize the jammer accurately. To provide sufficient security Elliptical Curve Cryptosystem (ECC) model is used.

INTRODUCTION:

The localization of deployed nodes is crucial especially in a wireless sensor network scenario. This is because the relevance of sensed data depends heavily on the availability of reliable sensor location data. For instance, with static wireless sensors monitoring the structural health of bridges, or buildings, abnormal sensor vibration readings are pointless if the location of the sensor is compromised. Locating the trouble spot becomes infeasible. Similarly, locating survivors using mobile wireless sensor networks requires that the sensors inform first responders that there is a survivor as well as provide a reliable estimate of his/her location. Consequently, given the importance associated with sensor location data, it is obvious that any attacks on this kind of data could jeopardize both the wireless sensor network and its intended application. Wireless networks make use of shared transmission medium. Therefore, they are open to several malicious attacks. An attacker with a radio transceiver intercepts a transmission, injects spurious packets, and blocks or jams the legitimate transmission. Jammer disrupt the wireless communication by generating high power noise across the entire bandwidth near the transmitting and receiver nodes. Since jamming attacks drastically degrade the performance of wireless networks, some effective mechanisms are required to detect their presence and to avoid them. Constant, deceptive, reactive, intelligent, and random jammers are few jamming techniques used in wireless medium. All of them can partically or fully jam the link at varying level of detection probabilities. Accurate detection of radio jamming attacks is challenging in mission critical in mission critical scenarios. Many detection techniques have been proposed in the literature, but the precision component is always an issue. Some of them either produce high false alarm rates or do partial detection of jammer attacks. Moreover, the results are based on simulations. After detection, classification of jammers

ISSN 2395-695X (Print)
ISSN 2395-695X (Online)
Available online at www.ijarbest.com
International Journal of Advanced Research in Biology Ecology Science and Technology (IJARBEST)
Vol. I, Special Issue I, August 2015 in association with VEL TECH HIGH TECH DR. RANGARAJAN DR. SAKUNTHALA ENGINEERING COLLEGE, CHENNAI
National Conference on Recent Technologies for Sustainable Development 2015 [RECHZIG'15] - 28th August 2015

attacksis necessary to launch appropriate recovery techniques like channel hopping or spatial retreat. The classification of jamming attacks play an important role not only differentiate them from each other but also to identify different network congestion or channel fading.

TYPES OF JAMMING ATTACKS:

a) Constant Jammers:

A constant Jammers continuously produce high power noise that represents random bits. The bit generator does not follow any media access control (MAC) protocol and operates independent of the channel sensing or traffic on the channel.

b) Random Jammers:

A random Jammers operates randomly in both sleep and jam intervals. During sleep interval, it sleeps irrespective of any traffic on the network, and during jam interval, it acts as a constant or reactive jammer. The jammer does not follow any MAC protocol. The PDR increases when the sleep interval increases and the packet size decreases.

c) Deceptive Jammers:

These jammers continuously send illegitimate so that the channel appears busy to the legitimate nodes. They are protocol aware and increase carrier sensing time for the legitimate nodes indefinitely. The difference between a decetive and a constant jammer is that a constant jammer sends packets with which appears legitimate to the receiver.

d) Reactive Jammers:

A reactive Jammers activates when it senses the transmission on the channel. If the channel is idle, it remains dormant and keeps sensing the channel. On sensing the transmission, it transmits enough noise resulting some sufficient number of bits corrupted in the legitimate packet so that packet checksum is not received by the receiver and the packet is discarded. Hence it causes the drop in PDR.

e) Shot noise intelligent Jammers:

Shot noised based intelligent jammers are protocol aware jammers that just beat forwarderror correction(EFC) scheme used at physical and MAC layers. The networks use conventional coding the physical layer. Single continuous pulse interfering legitimate packet can completely drop it if it is able to beat the FEC scheme used in the packet.

CHARACTERIZING JAMMING ATTACKS:

A Jamming attack can be detected easily, less effective, energy efficient or protocol aware.

There are a few commonly used metrics, characterizing the jamming attacks.

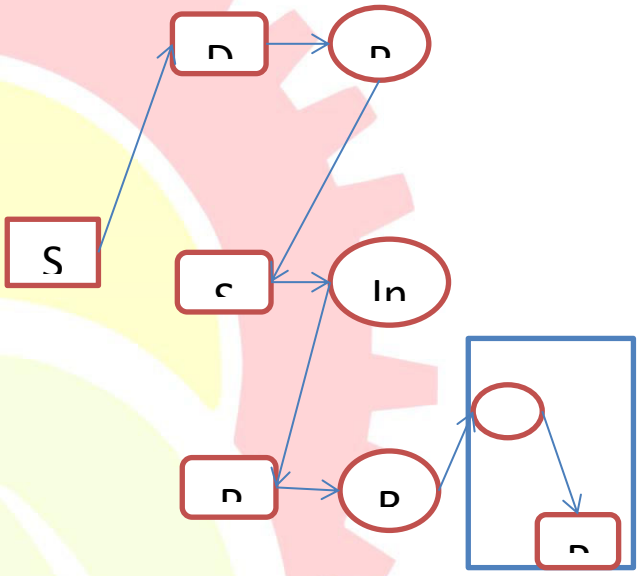
- Least detection probability.
- Stealthy against detectors.
- Completely denial of services like constant jammers.
- Protocol aware so that they are less likely to detect.

ISSN 2395-695X (Print)
ISSN 2395-695X (Online)
Available online at www.ijarbest.com
International Journal of Advanced Research in Biology Ecology Science and Technology (IJARBEST)
Vol. I, Special Issue I, August 2015 in association with VEL TECH HIGH TECH DR. RANGARAJAN DR. SAKUNTHALA ENGINEERING COLLEGE, CHENNAI
National Conference on Recent Technologies for Sustainable Development 2015 [RECHZIG'15] - 28th August 2015

- Authentication of users.
- Strength against FEC codes.
- Strength at physical layer to beat control channel coding techniques.
- Energy conservation is to get highest jamming efficiency with leat energy used.

EXISTING SYSTEM:

The existing system of the project is to find the jammer's location, using the indirect measurement scheme and the direct measurement scheme. The indirect measurement scheme uses "Received Signal Strength"(RSS). RSS is one of the most widely used measurements in localization. Received Signal Strength based approach to wireless localization offers the advantage of low cost and easy implementability RSS based localization problem may result in large errors due to the extra errors introduced when first estimating pairwise distance from the RSS measurements. In telecommunication, RSS is a measurement of the power present in a received radio signal. RSS is a generic radio receiver technology metric, which is usually invisible to the user of the device containing the receiver, but is directly known to users od wireless networking protocol family. The direct scheme uses the jamming signal strength to find the accurate position of the jammer. Estimating JSS is challenging as jamming signals may be embedded into other signals. As such, we devise an estimation scheme based on ambient noise floor and validate it with real world experiments. The ambient noise floor is the measure of signal created from the sum of all nodes and unwanted signal within a measurement system. To further reduce estimation errors, we define evaluation feedback metric to quantify the estimation errors and formulate jammer localization as a non-linear optimization problem.



DISADVANTAGES:

- High energy requirements and high probability of detection.
- No reliable communication.
- No adequate security.
- Easy to access the information.
- Errors due to the random nature of the fading channel, proximity measurements

PROPOSED SYSTEM:

ISSN 2395-695X (Print)
ISSN 2395-695X (Online)
Available online at www.ijarbest.com
International Journal of Advanced Research in Biology Ecology Science and Technology (IJARBEST)
Vol. I, Special Issue I, August 2015 in association with VEL TECH HIGH TECH DR. RANGARAJAN DR. SAKUNTHALA ENGINEERING COLLEGE, CHENNAI
National Conference on Recent Technologies for Sustainable Development 2015 [RECHZIG'15] - 28th August 2015

The indirect measurement scheme and the direct scheme uses receiving signal strength (RSS) and jamming signal strength (JSS) respectively to locate the accurate position of the jammer but does not provide adequate security. Hence to overcome this problem, Elliptical curve cryptosystem (ECC) model is used which provides security for data. ECC is an module system which uses encryption key for security. ECC is a public key encryption technique based on elliptic curve theory that can be used to create faster, smaller and more efficient cryprographic keys. ECC generated keys through the properties of the elliptic curve equation instead of the traditional method of generation as the product of very large prime numbers. According to some researchers ECC yield a level of security with a 164-bit key that other systems require a1024-bit key to achieve. Because ECC helps to establish equivalent security with lower computing power and battery resource usage, it is becoming widely used for mobile applications. ECC is based on the properties of the particular type of equation created from the mathematical group derived from points where the line intersects the axes. Multiplying a point on the curve by a number will produce another point on the curve, but it is very difficult to find what number will produce another point on was used, even if you know original point and the result. Equations based on elliptic curves have a characteristic that is very valuable for cryptography purposes.

ENCRYPTION:

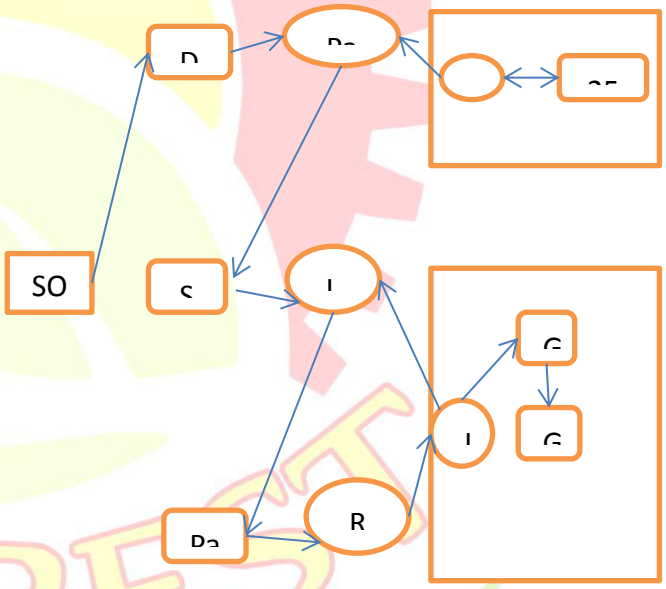
Encryption is a process of encoding message in such a way that only authorized parties can read.

PRIVATE KEY:

Private key is the one where only known parties can exchange information.

PUBLIC KEY:

Public key is a value provided by some designated authority as an encryption key that combines with a private key derived from public key that can be used in securing efficiently in messages or data.



ADVANTAGES:

- Provide efficient security for data.
- No acces of unauthorized users.
- More effective and more strength than the direct measurement scheme and the indirect measurement scheme.

ISSN 2395-695X (Print)
ISSN 2395-695X (Online)
Available online at www.ijarbest.com
International Journal of Advanced Research in Biology Ecology Science and Technology (IJARBEST)
Vol. I, Special Issue I, August 2015 in association with VEL TECH HIGH TECH DR. RANGARAJAN DR. SAKUNTHALA ENGINEERING COLLEGE, CHENNAI
National Conference on Recent Technologies for Sustainable Development 2015 [RECHZIG'15] - 28th August 2015

- Reliable communication in the wireless sensor network is provided.

- Minimization of the errors can be obtained.

LITERATURE SURVEY:

The title is Determining the position of the jammer using virtual force iterative approach is done by Hongbo Liu, Zhenhua Liu, Yingving Chen, WenyuanXu[5]. The disadvantages are Wireless communication is susceptible to radio interference and jamming attacks, which prevent the reception of communications. Anti-jamming works does not consider the location information of radio interferers and jammers. The advantages are to ensure availability of wireless networks. The next title is JAM: Jammed Area Mapping Service for Sensor Area Networks is written by Antony D.Wood, John A.Stankovic and Sang H.Son[2]. The disadvantages are, in wireless sensor networks is difficult primarily because of the limited reasources available to network nodes and the ease with which attacks are perpetrated. The advantages are, it reduces the failure rates on the wireless sensor networks. The localizing multiple jamming attackers in wireless networks is written by Hongbo Liu, Zhenhua Liu, Yingying Chen, WenyuanXu[8]. The disadvantages are, adversaries to build jammers with little effort to disturb network communication. The advantages are to ensure dependability of wireless communication, much work has been done to detect and defend against jamming attacks. The exploiting-Jamming caused Neighbour changes for Jamming Localization is written by Zhenhua Liu, HongboLiu,WenyuanXu and Yingying Chen[3]. The disadvantages are finding the position of the jammer will enable the network to actively exploit a wide range of defense strategies. The advantages are, it significantly reducesthe computation cost while achieving better performance. The Lightweight jammer localization in wireless network: System Design and implementation is written by KonstantinosPelechrinis, Lordanis, Koutsopoulos, LoannisBroustis, SrikanthV.Krishnamurthy[6]. The disadvantages are, a jamming device continuously emits electromagnetic energy on the medium. It dramatically increases the large number of packet collisions. The advantages are, a transmitter is thereby able to send more packets.

.

REFERNCES:

[1]Y. Zhang and W. Lee, 'Intrusion Detection in Wireless AdHoc Networks', 6th Int'l. Conf. Mobile Comp. and Net. Aug.2000, pp. 275-83.

[2]Antony D.Wood, John A.Stankovic and Sang H.Son "JAM: Jammed Area Mapping Service for Sensor Area Networks" IEEE Wireless Communications, February 2012,pp. 56-67.

[3]Zhenhua Liu, HongboLiu,WenyuanXu and Yingying Chen "exploiting-Jamming caused Neighbour changes for Jamming Localization" IEEE transaction on parallel and distributing system pp 547-555 2011[3]

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

ISSN 2395-695X (Print)
ISSN 2395-695X (Online)
Available online at www.ijarbest.com
International Journal of Advanced Research in Biology Ecology Science and Technology (IJARBEST)
Vol. I, Special Issue I, August 2015 in association with VEL TECH HIGH TECH DR. RANGARAJAN DR. SAKUNTHALA ENGINEERING COLLEGE, CHENNAI
National Conference on Recent Technologies for Sustainable Development 2015 [RECHZIG'15] - 28th August 2015

[5]Hongbo Liu • Zhenhua Liu • Yingying Chen • WenyuanXu "Determining the position of a jammer using a virtual-force iterative approach" 23 October 2010 springer

[6]KonstantinosPelechrinis, Lordanis, Koutsopoulos, LoannisBroustis, SrikanthV.Krishnamurthy "Lightweight jammer localization in wireless network: System Design and implementation" . In IEEE INFOCOM, 2011[6]

[7] Amitabh Mishra, KetanNadkarni, and AnimeshPatcha,Virginia Tech 'Intrusion Detection in Wireless Ad Hoc Networks', IEEE Wireless Communications, February 2004,pp. 48-60.

[8]Hongbo Liu, Zhenhua Liu, Yingying Chen, WenyuanXu "localizing multiple jamming attackers in wireless networks" IEEE Wireless nwteork, march 2013 pp 889-896

[9]Y. Huang, W. Fan, W. Lee, and P. S. Yu, 'Cross-Feature Analysis for Detecting Ad-Hoc Routing Anomalies',Proceedings of the 23rd IEEE International Conference on Distributed Computing Systems, 2003, pp. 478-487.

[10] Yu Liu, Yang Li and Hong Man, 'MAC Layer Anomaly Detection in Ad Hoc Networks', Proceedings of the 6th IEEE Information Assurance Workshop, June 17, 2005, pp. 402-409.

[11]B. Sun, K. Wu, and U. Pooch, 'Routing Anomaly Detection in Mobile Ad Hoc Networks', Proceedings of the 12th IEEE Int'lConf. on Computer Communications and Networks (ICCCN'03), Dallas, TX, Oct. 2003, pp. 25-3 1.

[12]Rena Hixon, Don M. Gruenbacher, 'Markov Chains in Network Intrusion Detection', Proceedings of the IEEE Workshopon Information Assurance, United States MilitaryAcademy, 2004, pp.432-433.

[13]Yia-an Huang, WEnke Lee, 'A Cooperative Intrusion Detection System for Ad hoc Networks', Proceedings of the Ist ACM Workshop on Security of Ad hoc and Sensor Networks, 2003, pp. 135-147.