Detection and Prevention of jamming attacks in wireless Networks

Neeti Malik

Dept. of Computer Science

ABSTRACT

In this paper, Jamming Attacks in context of a wireless network are discussed. Wireless networks are more vulnerable to jamming attacks because of their shared wireless medium. These attacks can be effectively executed by an aggressor by discharging radio recurrence signals. They endeavor to deny the client from utilizing accessible system assets. Jamming attacks are appalling Denial-of-administration attacks against the remote medium. In this paper, Different Types of Jammers that can be utilized to incapacitate the activity of remote systems and to avert these attacks, plans, for example, steganography, Data Hiding Schemes, DES are talked about. This paper likewise examines the answers for diminishing the jamming rate as well as to decrease the viability of jammer utilizing honeypot as an emergency course of action.

Keywords: Selective Jamming, DOS, Packet classification, Jammers.

INTRODUCTION

Networks are the series interconnection of nodes or points to transfer data through communicates media. The transmission medium is classified as wired and wireless technology. The wired technologies include coaxial cable, twisted pair cable and fiber optical cables. The wireless technologies include the radio waves, microwaves and infrared. Wireless communication is one of the fastest growing technologies and its demand is increasing dramatically. The network uses an electrical conductor. It permits even longer range communications, which is impossible for the wired technology. The types of wireless network are:

Wireless Personal Area Network (WPAN)

Wireless Local Area Network (WLAN)

Wireless Sensor Network (WSN)

Wireless Mesh Network (WMN)

Wireless Metropolitan Area Network (WMAN)

The correspondence range associated by one-to-numerous frameworks is called remote individual region systems (WPAN). The remote nearby system interfaces the short separation hubs and gives an inner access. The remote sensor system associates various sensor hubs, which are genuinely near one another. The remote work system is comprised of radio sign where the work topology is utilized. The system, which interfaces a few remote neighborhood systems, is called as the remote metropolitan territory systems (WMAN).

Wireless Sensor Networks

The sensor is spatially disseminated for checking nature condition, called as the remote sensor systems and its usage is expanded now-a-days. They are comprised of a few a large number of sensor hubs, which could convey remotely and the sensor hubs are little, lightweight and versatile. It is most well known in view of its simple establishment and decreased operational expense. The data could be moved anyplace with no association. The WSN is shaped by interfacing at least one sensor hubs. Every sensor hub in the system comprises of numerous segments, which incorporate transducers, microcontroller, handset, outer memory, control source and at least one sensors.

The transducer is in charge of creating electrical flag and after that the microcomputer procedure the information and stores it in the sensor yield. In the wake of accepting the direction from the base station, the handset transmits the information. A battery is utilized to provide food the sensor hubs. Since the remote sensor systems are occasion based systems, the hub which was left unattended for quite a while winds up dynamic when an occasion happens. The entrance to the systems is given by the numerous base stations, which go about as they brought together control.

The sensor hubs and base station hubs are the two sorts of hubs. The base station executes and deals with every one of the activities. Indeed, even once in a while without the assistance of base stations, the remote sensor hubs which are sent arbitrarily in a zone for perception would speak with one another. Sensor hubs, bunches, group head, base station are the basic piece of the remote sensor systems. So as to just the correspondence task the systems are grouped and the choice of bunch head happens for keeping up different hubs.

SECURITY OF WIRELESS SENSOR NETWORKS

In any condition, either physical or sensible, there exists the need of keeping up a person or thing safe away from damage. This is the job of security. On any PC related condition security can be considered as a non-useful necessity that keeps up the general framework usable and dependable, ensuring the data and data frameworks. Actually, in remote sensor systems, security is a vital significance. The system must be enough secured against noxious dangers that can influence its usefulness. Because of the job of sensor organizes as a "tactile framework", any aggravation in a sensor system may have results in reality. Be that as it may, accomplishing this objective isn't a simple assignment since sensor systems are particularly helpless against outside and inside attacks because of their unconventional qualities. The sensor hubs are exceptionally obliged as far as computational capacities, memory, and correspondence transmission capacity and battery control. Moreover, it is anything but difficult to physically access such hubs since they should be situated close to the physical wellspring of the occasions and they for the most part are not alter safe because of cost imperatives. Moreover, any inner or outside gadget can access to the data trade in light of the fact that the correspondence channel is open.

Therefore, sensor systems need to confront different dangers that may effectively obstruct its usefulness and invalidate the advantages of utilizing its administrations. These dangers to WSN can be sorted as pursues:

Common attacks

Denial of service attack (DoS)

Node compromise

Impersonation attack

Protocol-Specific attacks

Because of the highlights of sensor organizes there are some particular attacks focus in the correspondence channels. Like as pursues: Eavesdropping-A foe can without much of stretch recover profitable information from the transmitted parcels that are sent. Message Modification-That enemy can likewise essentially block and change the parcel's substance implied for the base station or middle of the road hubs. Message Replay-re-transmit the substance of those parcels sometime in the not too distant future. Message Injection-the aggressor can convey false information into the system, might take on the appearance of one of the hubs with the destinations of debasing the gathered sensor's perusing or upsetting the inner control information. Since sensor systems are remote administration arranged frameworks, one of the most risky attacks that they may face is the Denial of Service attacks (DoS). A DoS attack on a WSN may take a few structures.

Coming up next are most significant issues on WSN: Node cooperation - in which a lot of sensor hubs act noxiously and anticipate communicate messages from arriving at specific segments of the sensor organize, Jamming attack - in which an aggressor sticks the correspondence channel and maintain a strategic distance from any individual from the system in the influenced zone to send or get any bundle and Exhaustion of intensity - in which an assailant over and again demands parcels from hubs to drain their battery life. A sensor hub is considered as being undermined when an aggressor, through different methods can either peruse or change its inner memory. Attacks can be intrusive or non obtrusive. An obtrusive physical attack is characterized as an attack where the assailant physically breaks into the equipment by changing its equipment structure. Then again, a non-intrusive attack is characterized as an attack where the information is taken from the equipment gadget with no type of auxiliary change done to the gadget itself (for example exploiting the JTAG interface. Different complex attacks can be effectively propelled from traded off sensor hubs, since the subverted hub is an undeniable individual from the system.

Data Freshness Attack

In data freshness attack an adversary deliberately introduces a delay in the packet transmission or replays old messages to cause disruption in data aggregation.

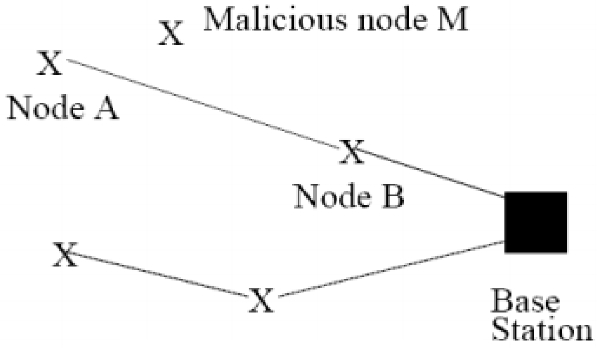

Fig. 1: Example of a malicious node

JAMMING TECHNIQUES

Jamming utilizes deliberate radio impedances to hurt remote correspondences by continuing conveying medium caught up with, making a transmitter back-off at whatever point it facilities occupied remote medium or undermined sign got at beneficiaries. Jamming generally targets attacks at the physical layer however once in a while cross-layer attacks are conceivable as well. In this segment, we expound on different kinds of jammers and the position of jammers to expand the stuck territory.

Types of Jammers

Jammers are vindictive remote hubs planted by an assailant to cause purposeful obstruction in a remote system. Contingent on the attack technique, a jammer can either have the equivalent or various capacities from real hubs in the system which they are attacking. The jamming impact of a jammer relies upon its radio transmitter power, area and effect on the system or the focused on hub. A jammer may jam a system in different approaches to make the jamming as compelling as could be allowed. Essentially, a jammer can be either basic or progressed relying on its usefulness. For the rudimentary jammers, we partitioned them into two subgroups: proactive and responsive. The propelled ones are additionally arranged into two sub-types: work explicit and shrewd half breed. The point by point characterization of various jammers can be found in Fig.2.

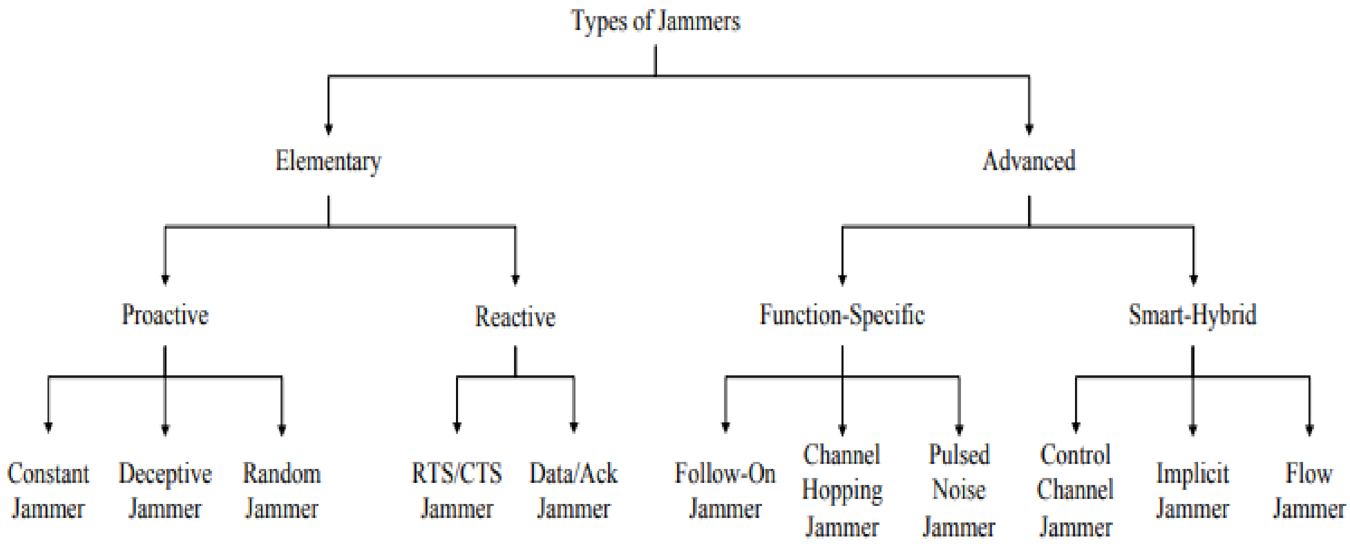

Figure 2: Types of jammers in wireless networks

Proactive jammer

Proactive jammer transmits jamming (interfering) signals whether or not there is data communication in a network. It sends bundles or arbitrary bits on the channel it is working on, putting all the others hubs on that direct in non-working modes. In any case, it doesn't switch channels and works on just one channel until its vitality is depleted. There are three fundamental sorts of proactive jammers: steady, beguiling and arbitrary. From here on, at whatever point we utilize proactive jammers it can mean all these three.

Constant jammer

Constant jammer transmits persistent, irregular bits without following the CSMA convention. As indicated by the CSMA component, a real hub needs to detect the status of the remote medium before transmitting. In the event that the medium is ceaselessly inert for a DCF Interframe Space (DIFS) length, at exactly that point it should transmit an edge. In the event that the channel is discovered occupied with during the DIFS interim, the station ought to concede its transmission. A steady jammer keeps real hubs from speaking with one another by making the remote media be continually occupied. This kind of attack is vitality wasteful and simple to identify however is exceptionally simple to dispatch and can harm organize correspondences to the point that nobody can impart whenever.

Deceptive jammer

Deceptive jammer ceaselessly transmits normal bundles rather than producing arbitrary bits (as in steady jammer). It misdirect different hubs to accept that an authentic transmission is occurring with the goal that they stay in getting states until the jammer is killed or bites the dust. Contrasted with a steady jammer, it is increasingly hard to identify a tricky jammer since it transmits genuine parcels rather than arbitrary bits. Like the steady jammer, tricky jammer is additionally vitality wasteful because of the nonstop transmission yet is effectively executed.

Random jammer

Random jammer irregularly transmits either irregular bits or standard bundles into systems. In opposition to the over two jammers, it targets sparing vitality. It persistently switches between two states: rest stage and jamming stage. It does for a specific time of period and after that ends up dynamic for jamming before returning back to a rest state. The resting and jamming time spans are either fixed or irregular. There is a tradeoff between jamming adequacy and vitality sparing on the grounds that it can't stick during its dozing period. The proportions among dozing and jamming time can be controlled to modify this tradeoff among proficiency and viability.

Reactive Jammer

Reactive Jammer starts jamming just when it watches a system movement happens on a specific channel. Accordingly, a responsive jammer focuses on trading off the gathering of a message. It can disturb both little and huge measured parcels. Since it needs to always screen the system, responsive jammer is less vitality productive than irregular jammer. Be that as it may, it is considerably harder to identify a responsive jammer than a proactive jammer in light of the fact that the bundle conveyance proportion (PDR) can't be resolved precisely by and by. As per (Pelechrinis et al, 2011), coming up next are two unique approaches to actualize a receptive jammer.

Function-specific Jammers

Function-specific jamming is executed by having a pre-decided capacity. Notwithstanding being either proactive or responsive, they can either take a shot at a solitary channel to monitor vitality or jam different channels or amplify the jamming throughput regardless of the vitality utilization. Notwithstanding when the jammer is jamming a solitary channel at once, they are not fixed to that channel and can change their channels as indicated by their particular usefulness.

Follow-on jammer

Follow-on jammer jumps over every single accessible channel as often as possible (thousand times each second) and sticks each channel for a brief time frame. On the off chance that a transmitter identifies the jamming and switches its channel, the pursue on jammer will examine the whole band and quest for another recurrence to stick once more. Or on the other hand, it might pursue a pseudo-arbitrary recurrence jumping succession. This kind of jammer saves control by restricting its attack to a solitary channel before bouncing to another. Because of its high recurrence bouncing rate, the pursue on jammer is especially compelling against some enemy of jamming procedures, for example recurrence jumping spread range (FHSS) which uses a moderate bouncing rate.

Channel- hopping jammer

Channel- hopping jammer jumps between various channels proactively. This kind of jammer has direct access to channels by superseding the CSMA calculation given by the MAC layer. In addition, it can stick numerous channels simultaneously. During its revelation and vertex-shading stages, the jammer is peaceful and is imperceptible to its neighbors. At that point, it starts performing attacks on various channels at various occasions as indicated by a foreordained pseudorandom grouping.

CONLUSION

In this study on jamming and against jamming strategies in remote systems, we have contributed by grouping and outlining different methodologies and talking about open research issues in the field. Various jammers attack remote systems in different ways so their attack impacts are altogether extraordinary. For example, a steady jammer expends all assets accessible and persistently sticks the system, however it is effectively identified. Then again, a responsive jammer detects the medium and possibly attack when a specific condition is fulfilled, so it is a decent decision for asset compelled equipment. In conclusion, if a jammer is an occasional low control one, it is difficult to be identified; an amazing jammer will unquestionably stick the greater part of the systems yet will be effectively recognized. The author likewise explores the position of jammers which is viewed as supportive in making jamming progressively compelling. For instance, to accomplish a superior jamming impact, it is conceivable to diminish the intensity of jammers by strategically setting them in the impedance scopes of conveying hubs. Regardless of how brilliant or compelling a jammer is, there is constantly at least one relating hostile to jamming strategies.

REFERENCES

[1] Neha Thakur, Aruna Sankaralingam “Introduction to Jamming Attacks and Prevention Techniques using Honeypots in Wireless Networks” in IRACST April 2013.

[2] Alnifie G, Simon R (2010) MULEPRO: a multichannel response to jamming attacks in wireless sensor networks. Wireless Communications and Mobile Computing 10(5):704–721

[3] Bayraktaroglu E, King C, Liu X, Noubir G, Rajaraman R, Thapa B (2008) On the performance of IEEE 802.11 under jamming. In: IEEE the 27th Conference on Computer Communications, pp 1265–1273.

[4] B. Thapa, G. Noubir, R. Rajaramanand, B. Sheng. On the robustness of IEEE802.11 rate adaptation algorithms against smart jamming", In Proceedings of WiSec, 2011.

[5] Y. Liu, P. Ning, H. Dai, A. Liu, "Randomized differential DSSS: Jamming-resistant wireless broadcast communication", In Proceedings of INFOCOM, San Diego, 2010.

[6] C. P¨opper, M. Strasser, S. Capkun, "Jamming-resistant broadcast communication without shared keys", In Proceedings of the USENIX Security Symposium, 2009.

[7] Y. Liu, P. Ning, H. Dai, A. Liu,"Randomized differential DSSS: Jamming-resistant wireless broadcast communication", In Proceedings of INFOCOM, San Diego, 2010.

[8] SciEngines. Break DES in less than a singleday, [Online] Available: http://www. sciengines.com, 2010.

[9] M. Strasser, C. P¨opper, S. Capkun, "Efficient uncoordinated fhss anti-jamming communication", In Proceedings of MobiHoc, pp. 207– 218, 2009.

[10] T. X. Brown, J. E. James, A. Sethi. Jamming and sensing of encrypted wireless ad hoc networks", In Proceedings of MobiHoc, pp. 120–130, 2006.

[11] M. Cagalj, S. Capkun, J.-P. Hubaux, “Wormhole-Based Anti Jamming Techniques in Sensor Networks”, IEEE Trans. Mobile Computing, Vol. 6, No. 1, pp. 100-114, Jan. 2007.

[12] R.C Merkle, secure communications over insecure channels. Communications of the ACM,21(4):2994-299,1978.