International Journal of Engineering Research in Electronic and Communication Engineering (IJERECE) Vol 3, Issue 5, May 2016

Solution for Jamming Attacks in Wireless Networks Using Time Delay Broadcasting

[1] Pranitha.S [2] Dr. Geetha .D
[1][2]School of Electronics and Communication Engineering
Reva University, Bangalore-560064
[1] pranithasriram.92@gmail.com [2] dgeetha@revainstitution.org

***Abstract*— We address the issues on broadcast communications due to jamming, considering a model which has trouble due to inside jammers. We consider a method for broadcasting messages from a trusted central authority based on the time and frequency named time-delayed broadcasting scheme (TDBS), which operates by transmitting a message one after the other serially to be broadcasted, transmission is based upon frequency and time slot. Their design prevents the leak of information due to the exposure of sequences by compromised nodes. This paper deals with the mechanism based on the traditional anti-jamming techniques which deal with spread spectrum(SS) concept to provide the communication which is jamming resistant in the presence of inside jammer through sequential and assisted broadcasting modes.**

***Keywords*— jamming, broadcast, compromised nodes, spread spectrum.**

I. INTRODUCTION

Wireless communications are susceptible to interference attacks which are intentional, known as jamming. Jamming in the simple terms is the adversary interfering with the signal reception by transmitting a continuous jamming signal or many jamming pulses [11]. Traditional systems used to prevent jamming use the concept of spread spectrum more in common. The methods used are Direct Sequence SS technique (DSSS) and Frequency Hopping SS technique (FHSS). Considering a pseudo-noise code which is responsible for bit spreading which provides protection bit by bit in SS method, which is secret and only nodes which communicate each other has the knowledge of it. The message from the sender should be broadcasted to all the receivers which is in the PN code form. The jamming prevention method, considering a system troubled by a internal jammer has been dealt by many researchers [3,6,7,9,10]. Through the exchange of broadcast messages they also exhibit coordination [5,8]. Time Delayed Broadcast Scheme is modeled to provide transmission of a message during a jammer is inside the system and coordination channel being absent.

The main steps in DSSS communication are as follows, if a given message has to be sent encoding it using Error correction code, the actual message is multiplied with a spreading code and sent through the sender. In the message each and every bit later on is converted to a chip sequence, according to the spreading code. The output obtained undergoes modulation and we up-convert it to the carrier frequency and send it through the channel. On the receiving end, the manipulated signal is down-converted to baseband, then it is demodulated and then despread by using a copy of synchronized spreading code. This synchronization has both bit time and chip time synchronization within it, provided that receivers are aware of which spreading code to apply based on the situation to get the original data back. On the other hand, a DSSS system can even perform the modulation prior to spreading process. The signal received is despread and then we perform demodulation.

Frequency hopping method from Spread Spectrum technique is concerned with the radio signal transfer by altering the carrier quickly among the different frequency bands. Using a common algorithm known to the transmitter and receiver both. Frequency hopping SS has various benefits in Wireless Sensor Networks, which minimizes jamming of radio signal transmission among the nodes. For the carrier, the SNR required decreases if a transmission uses wider frequency range. Numerous sensor networks can exist within the common location with no disturbance from the other unwanted signals. The main disadvantage of this method is bandwidth overall is more broader than the required one to send the same data using a single carrier frequency. Anyhow, transmission lasts over a limited period of time in each frequency, hence the frequency will be not occupied for long duration.

1.1 Types of Jammers:

Jammers are the malicious nodes in wireless communication, implanted by an attacker in order to cause an interference which is intentional in a wireless network. Based on the strategy of attacking, a jammer can exhibit the same or different features compared to the legitimate nodes in the network which they attack. The jamming effect observed due to a jammer is based on its radio transmitting power, location and influence on the network or the node being targeted. A jammer can jam a network in different ways to facilitate the effective jamming as much as possible. Mainly, a jammer can be classified depending upon its functionality as either elementary or advanced. The elementary jammers, are divided into two subgroups namely proactive and reactive. The function-specific and smart-hybrid are the two sub-types which are categorized from the advanced jammers.

This paper is organized as follows, In section 2 we provide the related work information. Basic overview is discussed in section 3, which deals with the main ideas, modes of operation to facilitate jamming- resistant communication. Section 4 gives the system and adversary models description. Steps in the broadcast modes are dealt in section 5. Section 6 deals with the results and finally conclusion is put forth in section 7.

II. RELATED WORK

The authors [3], proposed Keyless jam resistance which is concerned with the problem of jam resistance without key, considered to be important. There is a great demand for a system that broadcast messages between the sender entity and receiving entity without sharing any secrets previously. In the work mentioned, we make use of BBC algorithm. We study a problem in ad hoc networks based on multi-channel concept for jamming attacks in control-channel. We also have a scheme named DSSS-based broadcast communication, defending in opposition to inside Jammers using Delayed seed-disclosure [2]. There is a scheme which proposes a broadcast communication which is jamming-resistant without using shared keys which is very essential for critical-safety applications. We study a work which proposes, Mitigation of jamming for control channel through random key distribution.

We consider the target of a attacker is to broadcast the channel, which reduces power required for the performance of DoS attack [4]. We have a scheme which is a jamming-resistant technique and saves the message broadcasted from inside and colluding jammers which are small in number [7]. The method depends on the design which let the secret information sharing partially, based on the location of the frequency bands which facilitate broadcast operation. Other substitute methods remove the dependency on the shared secrets [3,9,10]. The method with not using a key, we study a system which prevents jamming [3]. A solution from Uncoordinated Direct Sequence SS (UDSSS) method, where a message to be broadcasted use PN code for spreading according to a set of codes selected randomly from a public code book. The work put forth a RD-DSSS, a randomized differential DSSS technique which is also dependent on PN codes which are selected at random [10]. In the case of reactive jammers resilience is achieved better in RD-DSSS scheme compared to UDSSS.

III. BASIC OVERVIEW

To achieve the communications which provide a jamming-resistant system when insiders are present. TDBS presents a broadcasting scheme which is a series of unicast transmissions defined in terms of both frequency and time slot, hence preventing the merging of each and every node on a frequency channel used in common. Each node knows its schedule, the unicast transmissions locations are defined using a frequency band and a time slot (f,s) in which all nodes knows it partially. Hence, the locations of other nodes which are communicating are kept secret but leaks the set of locations belonging to the node which is being compromised only. To serve this need, scheduling of nodes is done which facilitate communication over frequency bands selected randomly by dividing the nodes into pairs. In order to provide less flexibility for a node which is compromised, we can also divide the set of nodes in to groups to provide the broadcast communication which is efficient. Since we deal with the property of preventing jamming, we take the condition of joining two nodes resulting in pairing into account first. In a FH system the node pairs which communicate and the frequency bands which are assigned change on a basis of per-slot.

Two modes in which TDBS operates are Sequential Unicast mode (SU) and Assisted Broadcast mode (AB). SU mode operates as, the sender sends the information serially to receivers which are intended. This mode is not an efficient mode and is applied when the receivers has no capacity to transmit further anymore or the receiver is not trusted to pass the information to be broadcasted. A node which receives a message to be broadcasted can be used as a relay for that message in the AB mode.

3.1 Existing And Proposed System:

Disadvantages of existing system: The broadcast involves all the receivers to be tuned to the same channel typically, only then the reception of the message can be assured. Jammers can receive the information which is broadcasted

due to which the overall network resources are spoiled. The process is unauthorized because delivering of data has no guarantee.

Advantages of proposed system: The broadcast scheme proposed is efficient since it resists the jammer in wireless network by providing a guaranteed delivery of message to all the intended receivers. The battery power of nodes is not spoiled, but a time delay which is small will occur during the message delivery, which has to be broadcasted. Nodes are allocated with different channels dynamically to receive the data with more number of channels.

IV. SYSTEM AND ADVERSARY MODEL

***System Model*:** Initiation for the broadcast transmissions can be done by any node to its neighbors. We consider that the network is divided into clusters to form cliques. For this design, broadcast transmissions are restricted within a cluster, or can be propagated to other clusters also. We consider, frequency hop will occur on the basis of per-slot. We consider that, the transmission of one message unit requires one time slot of duration which is assumed to be enough. Initialization of network begins through a Central authority, which priorly loads the necessary values like frequency hop patterns and various other secrets in cryptography.

Threat Model: We may think that some receivers may be compromised by an attacker, which may result in exploiting any secret they send from sender to the other receivers to jam the communication. We consider the jammers which are brilliant and know the methods which we follow. In order to disturb the broadcast communication, the jammer modifies or injects the messages which are meaningful along with injecting the random noises.

***Adversary Model*:** The main aim of the opponent is to avoid the transmission of information from sender to a set of predetermined receivers. In order to carry out this, the adversary plants a few jamming devices choosing particular locations on his own, which could be synchronized centrally. The devices so implanted, according to the adversary's choice jam any J frequency bands collectively with the addition of interfering signals for the frequencies selected. Frequency bands which are jammed provides wireless transmissions which are corrupted and irrecoverable. The adversary has a capacity of compromising the devices in the network physically and can recover the information which is stored along with the keys using cryptography, PN codes etc. Adversary knows the various methods to guard the broadcast communications even.

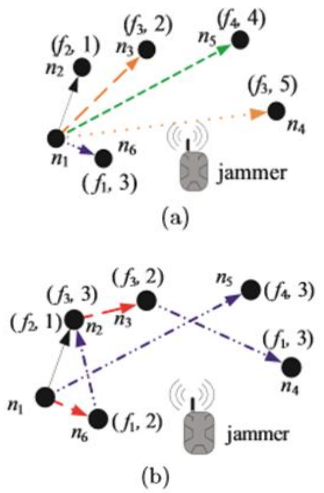

Figure 1: (a) SU mode of Operation. (b) AB mode of Operation.

V. STEPS IN UNICAST AND BROADCAST MODES

Designing the frequency hop sequences for the individual nodes is the main challenge for the TDBS system in such a way the following requirements should be satisfied (1) sequences should be pseudo-random (b) subset of nodes compromised will not reveal the information related to the nodes which are not compromised and (c) each node is given equal chance for performing the broadcast. We formulate few steps in order to construct the hopping sequences for SU mode and AB mode in this section, which satisfies the above mentioned requirements.
Sequential Unicast Mode: Here, a sender transmits the message which is to be broadcasted in a sequential fashion to (2n −1) receivers which are intended. For the SU mode, construction of the hopping sequence follows the steps as explained below,

Step-1: Construct a 1-factorization for F2n number of nodes.
Step-2: For all Fi belonging to F2n, where "i" ranges from $0 \le i \le 2n-2$, perform the Steps 3–5.
Step-3: Get a random permutation π for the set of frequency bands.
Step-4: Allocate bands of frequency in π to edges of Fi in array of edges.
Step-5: Perform Steps 3 and 4 till all node pairs in Fi are given a band of frequency.
Step-6: Perform the Steps 1-5.

***Assisted Broadcast mode*:** This mode explains that, node with a message facilitates the further message broadcast

which functions as relay for broadcasting. Hence the delay is minimized by this property, until the completion of broadcast operation, meanwhile causing resilience to jamming. For constructing the hop pattern in this method we use the steps as follows,

Step-1: Fetch a arbitrary 1-factor F0 of nodes. Initially consider the value of i as 0.
Step-2: Get a permutation "π" of the set of frequency bands, which is random.
Step-3: allocate bands in "π" to edges with Fi, in the order of which edges occurr.
Step-4: Perform Steps-2 and 3 till all node pairs in Fi are assigned with a band of frequency.
Step-5: Build a 1-factor Fi+1, on the basis of splitting algorithm. Set the value of i = i +1 .
Step-6: Perform Steps-2 and 5.

VI. RESULTS AND DISCUSSION

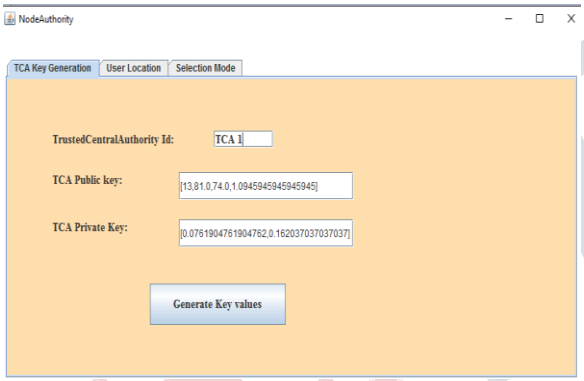

Figure 1: TCA key generation

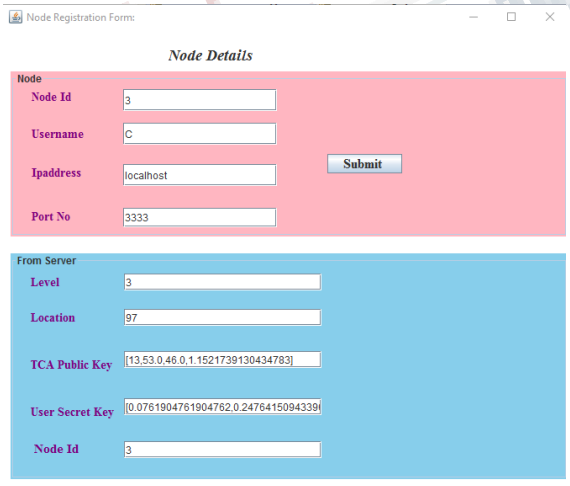

Figure 2: Registration of the node

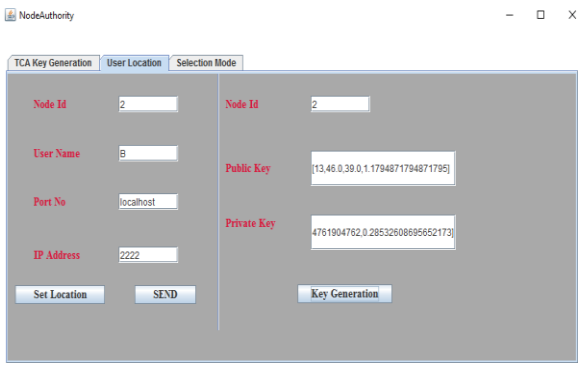

Figure 3: To set the location from server

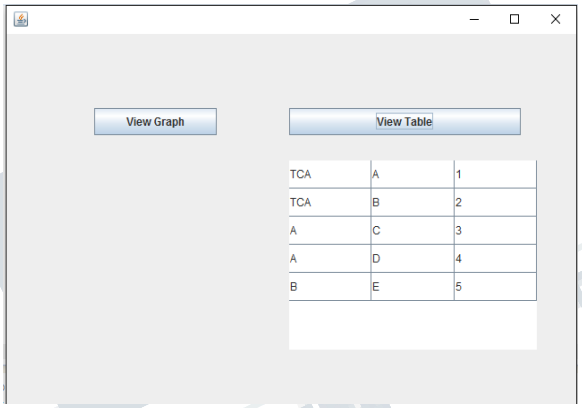

Figure 4: Table showing node connections

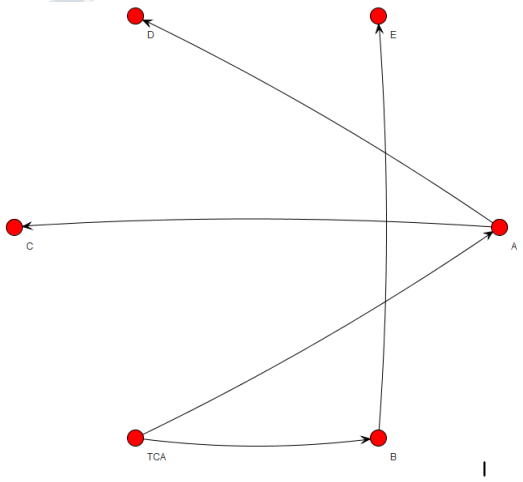

Figure 5: Diagram showing node connections

The results obtained are as shown above, Figure 1 shows the generation of key values for trusted central authority, with both public and private key values. Figure 2 provides the node registration details including the assignment of

username and node Id. Location for the nodes is been set in the Figure 3, from the server. Figure 4 and 5 represents the node connection details in the table and diagram form respectively.

VII. CONCLUSION:

Based on this paper, we deal with the conventional anti-jamming techniques, types of jammers, a scheme which provides a jamming-resistant communication. The system operates in such a way that if a node surrenders for jamming technique, it leaks only a partial information present with it, making the other communicating nodes secure which are uncompromised. In order to facilitate this, nodes are grouped together forming a pair with each other which are assigned with the frequency channels for communication process selected randomly, through the sequential unicast and assisted broadcast mode of operation, considering frequency and time when jammers are present inside the system. Hence providing a jamming-resistant property.

REFERENCES

[1] S. Liu, L. Lazos, and M. Krunz, "Thwarting inside jamming attacks on wireless broadcast communications," in Proc. 4th ACM WiSec Conf., 2011, pp. 29–40.

[2] A. Liu, P. Ning, H. Dai, Y. Liu, and C. Wang, "Defending DSSS based broadcast communication against insider jammers via delayed seed-disclosure," in Proc. Annu. Comput. Secur. Appl. Conf., 2010, pp. 367–376.

[3] L. C. Baird, W. L. Bahn, M. D. Collins, M. C. Carlisle, and S. C. Butler. "Keyless jam resistance", in Proc. of the IEEE Workshop on Information Assurance United States Military Academy, 2007.

[4] A. Chan, X. Liu, G. Noubir, and B. Thapa. "Control channel jamming: Resilience and identification of traitors", in Proc. of ISIT, 2007.

[5] P. Chaporkar, K. Kar, X. Luo, and S. Sarkar. "Throughput and fairness guarantees through maximal scheduling in wireless networks". IEEE Transactions on Information Theory, 54 (2), pp. 572–594, 2008.

[6] J. T. Chiang and Y.-C. Hu. "Dynamic jamming mitigation for wireless broadcast networks", in Proc. of INFOCOM, pages 1211–1219, 2008.

[7] Y. Desmedt, R. Safavi-Naini, H. Wang, C. Charnes, and J. Pieprzyk. "Broadcast anti-jamming systems", in Proc. of the IEEE International Conference on Networks (ICON), pages 349 – 355, 1999.

[8] A. Gupta, X. Lin, and R. Srikant. "Low-complexity distributed scheduling algorithms for wireless networks". IEEE/ACM Transactions on Networking (TON), 17(6):1846–1859, 2009.

[9] L. Lazos, S. Liu, and M. Krunz. "Mitigating control-channel jamming attacks in multi-channel ad hoc networks". In Proc. of WiSec, pages 169–180, 2009.

[10] Y. Liu, P. Ning, H. Dai, and A. Liu. "Randomized diff erential DSSS: Jamming-resistant wireless broadcast communication", in Proc. of INFOCOM , 2010.

[11] G. Noubir and G. Lin. "Low-power DoS attacks in data wireless LANs and countermeasures". Mobile Computing and Communications Review, 7(3):29–30, 2003.