Avoidance of Indoor Jammers using Instance Belated Diffusion

C. Saravanan
M.E. Student
Department of Computer Science & Engineering
Arunai Engineering College, Tamilnadu, India

Abstract— Wireless communication is exposed to signal jamming attacks. Spread spectrum mitigates such problem by scattering narrowband signals over an much wider band frequencies and forcing jammers. In broadcast systems, jammers can easily find out the spread pattern by some receivers. In most wireless networks, nodes can only be limited local information about the state of the network. Wireless networks have the characteristics of broadcast, which brings the nuisance for illegal users to interfere the network or even attack the network. Therefore a series of network problems arise. The open nature of wireless network leaves it to malicious threats. We address the problem of jamming-resistant broadcast communications. For a jamming scene with one transmitter, one receiver and a jammer In the literatures of both eavesdropping and jammer, the threats are caused by the single malicious jammer. In a supplementary analysis, the transmitter and the malicious jammer relay can select the appropriate rate to send signals to increase or reduce the secrecy rate. Wireless networks enable a wealth of commercial, tactical and social applications ranging from single point to point voice communications, information retrieval, monetary transactions, environment monitoring, social networking, navigation and jamming. Many of these applications target users who access the numerous network services via their devices. We propose time-delayed broadcast scheme (TDBS) which makes the broadcast in an unicast communication series. Each node follows an unique pseudo-noise (PN) frequency hopping sequence. We map the problem of constructing PN sequences to the 1-factorization problem for complete graphs. We also accommodate dynamic broadcast groups by mapping the updating the assigned PN sequences.

Key words: Instance Belated Diffusion, Indoor Jammers

I. INTRODUCTION

Wireless networks are susceptible to threats due to the open nature of the wireless medium. Broadcasting provides an economic way of disseminating a copy of the same message to multiple receivers using a single transmission. One severe form of Dos attack is jamming. In this, we investigate and alleviate the impact of jamming attacks on broadcast communications in the presence of inside adversaries. We develop several communication protocols that protect the broadcast communication from Dos attacks. Over the last decades, wireless communications proved to be an enabling technology to an more number of applications.

The wireless network and its support of mobility has revolutionized the way we access the data, information services and interact with the physical world. Wireless technology has been widely used in cyber-physical system such as air-traffic, control, power plants synchronization. To provide an service in a wireless network user data and application control data. Jam resistance is increasingly important to modern communication. In wireless networks the jamming attack is the most vulnerable attack, in which jammers interrupt our transmission by sending their jamming signal. The existing methods to overcome the jamming attacks are spread spectrum techniques which include direct sequence and frequency hopping.

In frequency hopping sequence, the sender and receiver communicate on a single frequency for a short peroid, then jump to another frequency. Bluetooth uses this technique and changes frequencies every 0.25 ms. If the sequence of frequencies are determined by a secret key, then the attacker will not know which frequency to jam at any given time. A smart jammer can usually succeed by destroying only the portion of the message, which requires fewer frequencies to be jammed and requires less energy.

In direct sequence, sender uses all frequencies by combining the message with a pseudorandom bit stream generated to some key. This is used in CDMA (code division multiple access). If the civilian GPS signal used a key, then that key would have to be distributed to all users, including the attackers. Handheld jammers are been implemented for cell phones. Theoretically, cell phones are jam resistant by using a unique secret key for each customer. In conventional wireless communication, the information is modulated onto a proper high frequency carrier for transmission.

If the attacker (or jammer) injects relevant signals into the same spectral region, he can significantly reduce the signal-to-noise ratio(SNR) at destination which interrupt the wireless communication.

Wireless networks are susceptible to numerous security threats due to open nature of the wireless medium. Anyone with a transceiver can eavesdrop on the ongoing transmissions, inject malicious messages, or block the transmission. Degrading the network performance is by jamming wireless transmission. In the simplest form of jamming, the sender affects the transmitted messages by causing electromagnetic interference in the network's operational frequencies and to the targeted receivers.

Denial of service(Dos) aims at filling user-domain and kernel-domain. Due to shared data, an adversary called Jammer can easily interfere the wireless communication using radio frequencies by transmitting a great deal of unmeaning signal disregarding MAC protocols. A variety of jamming attacks can be performed to interfere the wireless communication channel. The most efficient attacks can be reduce into four type:

- Constant Jammer: Continually send random and meaningless signal to the channel.
- Deceptive Jammer: Send valid packets which means a packet header with a useless payload.
- Random Jammer: Alternate between jamming and sleeping mode. In detail, the jammer performs constant jammer or deceptive jammer for a random period then shutdown the jammer for another random period of time.

– Reactive Jammer: This spent more energy on sensing the channel then damaged signal using minimum power.

To defend from jammers, the first step is to detect the presence of jammer such as low signal and low power. In this, we develop anti-jamming methods that adopt the frequency hopping spread spectrum design. It is used to exhibit a graceful degradation in performance with increase in interference.

A. Main Contributions

1) Mitigation of Control Channel Jamming From Internal Jammers

Organizing a collection of nodes into wireless networks require implementation of critical network functions such as channel assignment, routing and time synchronization. These functions are coordinated by exchanging messages on a broadcast channel known as the control channel. Networks deployed in hostile environments are susceptible to Dos attacks. A randomized distributed channel establishment and maintenance scheme is developed to allow nodes to establish a new control channel using frequency hopping.

2) Mitigation of Jamming In Broadcast Communication

Broadcast transmissions intend disseminate important messages like control information to a large set of nodes on a common channel known to all receivers.

3) Jamming Attacks In Wireless Networks

Jamming is an extensively studied topic in the context of wireless communications. Most prior research assumes that the jammer is an external entity, oblivious to the protocol specifics and cryptographic secrets.

4) Motivation

Typically, jamming attacks have been analyzed and addressed as a physical-layer vulnerability. The jamming techniques based on spread spectrum (SS). These techniques provide bit-level protection by spreading bits, known only to the communicating parties. To corrupt a SS signal, an adversary who is unaware of the PN code has to transmit with a power that is several orders of magnitude higher than the power of the SS transmission.

Hence, the adversary needs to stay active only for a fraction of the time required for a packet transmission. Moreover the control channel operates at a low transmission rate, significantly reduces the adversary's effort.

It was shown that to perform a DoS attack in GSM networks is reduced by several magnitude when the attack targets the control channel. Moreover, potential disclosure of cryptographic codes .

B. Our Contributions

We develop TDBS(Time delayed broadcast scheme) an emergency mechanism for restoring the broadcast communications temporarily until the inside jammers are removed from the network. It propagates broadcast messages as a series of unicast transmissions. The presence of inside jammers are known by the location of these unicast transmissions, defined by a frequency band or slot pair, are only partially known to any subset of receivers. Assuming that the jammer only interferes with a limited number of frequency band, a subset of the unicast transmissions are interference-free. The problem of FH sequences design is mapped to 1-factorization problem in complete graphs.

II. SYSTEM AND ADVERSIAL MODELS

A. Network Model:

Consider two network topology models such that it is typical in wireless LANs, personal area networks and in military scenarios, where the mobile coalitions move in a team-coordinated form. To make TDBS scalable with the network size, we assume the network is partitioned into clusters. We consider a wireless ad hoc network consisting of N nodes. The available spectrum channels may be fixed or may be dynamically assigned.

In the case of static spectrum assignment, the network is assumed to operate over a set C = {f1, . . . , fK} of K distinct frequency channels (e.g., K = 11−13 for 802.11 networks and K = 79 for 802.15 networks). In the case of runtime spectrum networks, the number of idle channels at time t, denoted by K(t), varies according to primary radio (PR) activity. In this case, the maximum number of idle channels is denoted by K. Cognitive radio (CR) nodes are used for determining the set of idle channels at any given time. Various sensing methods can be used for this purpose.

Each node is equipped with a half-duplex transceiver. Hence, a node can only listen to or transmit over one band at a time. Note that if communicating nodes are equipped with more complex hardware (e.g., multiple transceivers per node), the communication efficiency of our schemes and their resilience to jamming can be further improved. Without loss of generality, we consider a time-slotted system. Network nodes are assumed to be capable of slowly hopping between available channels. For simplicity,

We assume that one frequency hop can occur per time slot. The network is initialized by a trusted authority, which is used for default parameters such as pseudo-noise (PN) FH sequences and other cryptographic secrets. Prior trust has been established between network nodes. Neighboring nodes share pair wise symmetric keys that can be used for secure unicast communication. The communication can be a public or an private. In the latter case, confidentiality is done by efficient public key operations. Once the network is initialized, the trusted authority is no longer needed

B. System Model:

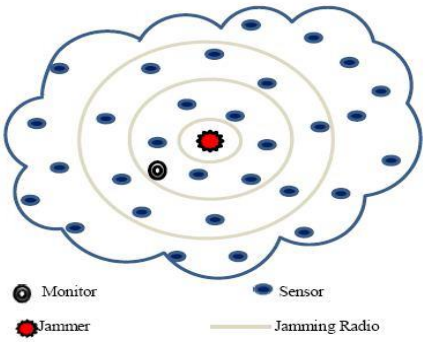

Fig. 1: System Model

The communication is of K non-overlapping frequency bands. Each node is equipped with a single half-duplex transceiver. All nodes are equipped with a GPS radio independently synchronized to a time-slotted system. Besides clock synchronization, nodes achieve frame synchronization using standard PHY-layer frame detection methods for FHSS systems.

C. Adversary Model:

This is mainly used for preventing the senders from communicating with all receivers or a subset of them. The jamming devices are based upon frequency bands on a per-slot basis. However, the jammer hopping rate is limited by the use of time to be maintained for a particular band. The jammer can target the frame synchronization process by jamming the preamble of a transmitted frame. The signal cross-correlation has been shown to have a high immunity to interference.

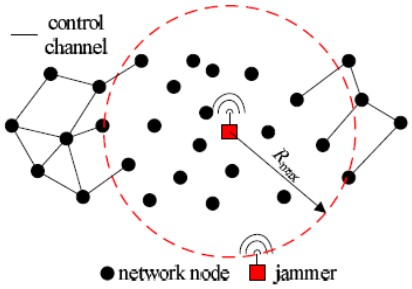

Fig. 2: Adversary Model

The system is capable of physically uniting the network devices and recovering stored information including cryptographic keys, PN codes, etc. To do so, the adversary deliberately interferes with transmissions on those bands within a jamming range Rmax.

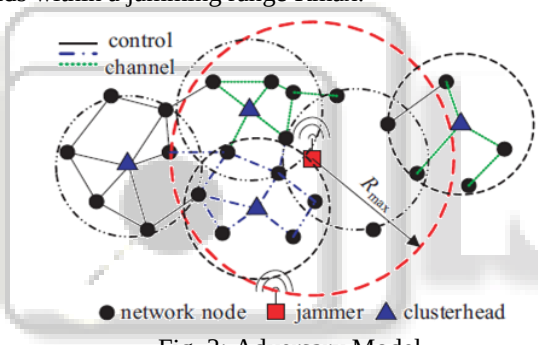

Fig. 3: Adversary Model

Messages received by any node within the jamming range and at the jammed frequency band are assumed to be corrupted. The nodes are capable of determining attacks if they are within distance Rmax from the jammer and are enabled with jammed frequency band.

To assume that the system can physically compromise network devices and recover the data such as PN codes. Note that with dedicated hardware, the jammer may be able to work at regular nodes. However, the jammer's hopping rate is limited in order to corrupt a sufficient number of bits from the targeted packet(s).

III. Overview of TDBS

The communications in the presence of inside jammers is been verified. Using frequency hopping spread spectrum (FHSS), we propose Time Delayed Broadcast Scheme (TDBS) for this type of communications. It differs from classical FHSS design in that two communicating nodes do not follow the same sequence, but are assigned a unique one that have high correlation properties. It implements the broadcast communication distributed in frequency and time. The locations of unicast transmissions defined by frequency and time are partially known to the receivers. Because the jammer can interfere only with a subset of frequency bands in a given time slot from a unicast transmissions. The problem of FH sequence design is mapped to 1-factorization problem in complete graphs. Hence it is not a replacement of conventional broadcast mechanism. Instead, it is an emergency mechanism to restore the communications temporarily until the jammers are been removed. TDBS can operate in two modes: the sequential Unicast mode(SU) and the Assisted Broadcast mode(AB). In SU mode, the sender relays information to intended receivers. In AB mode, any node that receives a broadcast message can act as a relay for that message. The main challenge in TDBS is to design the FH sequences of individual nodes for the following requirements: (a) hopping sequences are pseudo-random, (b) Compromise of a subset of nodes limits the information leakage and (c) Every node has the opportunity to perform a broadcast.

IV. System Architecture

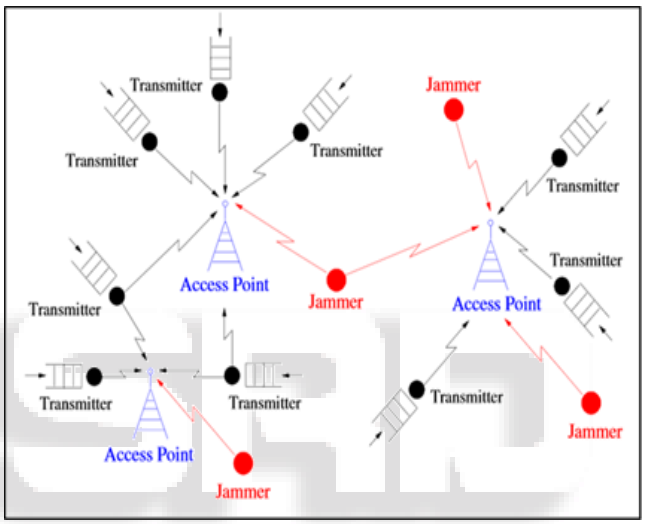

Fig. 4: System Architecture

A jammer is an electronic device or an machine which stay in between the user and the server and avoids threats by providing security. It is possible with the help of:

- Radio Frequencies
- FPGA

Radio frequencies play an important in jamming such that it is useful in preventing the targeted device from establishing or maintaining a connection in the network field. FPGA means Field Programmable Gate Array which is an integrated circuit that is to be configured by the customer or a designer that can be programmed by a user in order to give the security in the network.

V. Definitions and Useful Theorems

- Definition1: Complete graph: A graph G(V,E) with vertex set V and edge E is complete if each vertex pair is connected by an edge.
- Definition2: 1-factor: perfect matching F of graph G is a subset of E that partitions V and F is a set of pair wise disjoint edges of G.
- Definition3: 1-factorization: A 1-factorization $F_{2n} = \{F_0, F_1, \ldots, F_{2n-2}\}$ of an graph G is a partition of its edge set E to (2n-1) 1-factors.
- Theorem1: 1-factorization of k_{2n}: A complete graph k_{2n} is factorable.

A. TDBS-SU Sequential Unicast Mode

In the SU mode, a sender unicasts the broadcast message to (2n-1) receivers. Let p_k be the permutation set of C. The pseudocode for TDBS-SU is given in algorithm 1. We apply this algorithm to a four-node group, when C={$f_1,f_2,.....f_5$}, (k=5). Because K>=n, the n pairs corresponding to a 1-factor communicate in parallel in one slot.

The random permutation for F_0 is $\prod$ = {f2,f3,f5,f1,f4}. When k<n, parallel transmissions to 1-factor are distributed over multiple slots.

B. Algorithm 1 TDBS-SU: Sequential Unicast Mode

1) Generate F_{2n} of K_{2n}
2) repeat
3) for i = 0 to (2n - 2) do
4) for j = 1 to [n/k] do
5) π = rand(perm(C))
6) for w = 1 to min{n,k} do
7) $h_F((j-1)K+w,1) = h_F((j-1)K+w,2) = \pi(w)$
8) end for
9) end for
10) end for
11) end repeat

1) TDBS-AB Assisted Broadcast Mode

In the AB mode, any node that has already received a broadcast message operates as a broadcast relay. To construct FH hopping sequences for the AB mode, the 1-factors F_i are selected and arranged such that the number of nodes that can relay a broadcast transmission at each 1-factor is maximized.

– Definition4: Relay set R^i_j: The relay set R^i_j of a node v_j that originated a message m is defined as the set of nodes that can relay m in 1-factor F_i.

2) Algorithm 2 TDBS-AB: Assisted Broadcast Mode

1) Generate random F0 of K2n
2) initialize i = 0
3) repeat
4) for j = 1 to [n/k] do
5) π = rand(perm(C))
6) for w = 1 to min{n,k}do
7) hFi((j□1)K+w;1) = hFi((j-1)K+w;2) =π(w)
8) end for
9) end for
10) Fi+1 = split(Fi)
11) i + +
12) end repeat

VI. PERFORMANCE EVALUATION

Definition 5: Broadcast Delay D: Number of slots required until all broadcast group members have received a copy of the broadcast message. The broadcast delay is the inverse of the throughput achieved by the TDBS broadcasting operation. Although TDBS is designed for enabling broadcast in the presence of internal jammers, we can execute the per-node throughput in the absence of jamming.

A. Resilience to External Jammers

Under an external threat model, the FH sequences assigned to various nodes are assumed secrets. A jammer acting as an eavesdropper by randomly hopping on various channels would require many FH sequence periods to reconstruct FH sequence of a node. For the external jammer we assume that the adversary deploys multiple jamming devices that can jam up to J frequency bands per time slot, with J < K.

B. Resilience to Internal Jammers

We assumed that the adversary has compromised r nodes and recovered their FH sequences. we are interested in determining the broadcast delay until the remaining (2n-r-1) legitimate nodes receive a broadcast message m.

VII. EVALUATION OF MULTIHOP SCENARIOS

We evaluate TDBS for multi-hop networks and to be focused on the anti-jamming-resistance of the inter-cluster phase. For the inter-cluster phase, we define the following metrics.

– Definition 6: Flooding Delay D_f: Number of slots needed until all clusters adjacent to a cluster x, have received a broadcast.
– Definition 7: Escape Delay D_e: Number of slots needed until a broadcast message that originated at a cluster x is received by any node in any adjacent cluster.
– Definition 8: Escape Diversity DIV: Fraction of adjacent clusters that receive a broadcast directly from a cluster x, when a subset of the border nodes in x are compromised.

VIII. RELATED WORK

The jamming is typically mitigated by spreading the transmitted signal to a larger bandwidth using the secret PN code. we addressed the problem of selective jamming and their attacks in wireless networks. We consider an internal threat model in which the jammer is a part of an network.

Wireless networks have been developed into many forms such as ad hoc networks and wireless sensor networks. Receiver must exhaustively apply all codes in the codebook to recover the broadcast message. DSSS-based schemes are not directly comparable with TDBS because they employ different physical-layer mechanisms for rejecting narrowband interference.

DSSS communications are resilient to low/medium interference levels. Several methods attempt to identify the compromised nodes that leaked information to the jammer. Lazos et al. proposed the assignment of unique FH hopping sequences to each receiver. Chiang and hu developed a code-tree approach for identifying PN codes.

IX. CONCLUSION

We proposed TDBS, a scheme for jamming - resistant broadcast communications in the presence of inside jammers.

In TDBS, broadcast is done as a series of unicast transmissions distributed in frequency and time. The adversary is limited with number of channels such that the interference is increased and the corresponding bandwidth is decreased. We mapped the problem of minimizing FH sequence changes needed for node addition or deletion. We analytically evaluated the security properties of TDBS under both internal and external threat model and shown that it maintains broadcast communications even when multiple nodes are used.

X. FUTURE WORK

When jamming attacks detection is completed, the information on the jamming types may be used as two parts: jamming defense and jamming localization. Jamming defense is used to decrease the influence of jamming attacks and to keep the communication connected. While the jamming localization was used to lock the position of the jammer.

One of the most popular strategies used in wireless networks is channel surfing. It is implemented by changing the communication frequency to a range avoiding the interference from the adversary. Another method is Spatial Retreats which can be achieve by moving the wireless users to a new area where no interference exists.

Future wireless networks face many technical challenges related to the limited spectrum availability, the unreliability, and open nature of the wireless medium. Key problems include the scalability, reliability, availability, resource-efficiency and security of the networking elements and of the information that they carry. These problems oftentimes pose competing design goals that require the establishment of trade-off mechanisms.

One such design tradeoff is the purpose of security and network availability in the presence of threats versus resource-efficient network operation. The former is critical for ensuring uninterrupted access to network services, while the latter is necessary for prolonging the lifetime of battery operated devices. Trading resource-efficiency for security and reliability is, in most cases, inevitable since implementation of any sort of security mechanism requires the dedication of resources.

REFERENCES

[1] Performance Analysis of Physical Layer Security under the Cooperation of Multiple Malicious Jammer Relays Shengbin Lin, Qingfeng Liu, Kaizhi Huang, and Wen Wang, International Journal of Computer Science and Electronics Engineering (IJCSEE) Volume 3, Issue 2 (2015).
[2] Securing Wireless Broadcast Communications against Internal Attacks, By Sisi liu, Department of electrical and computer engineering, University of arizona, 2012.
[3] C. Po¨pper, M. Strasser, and S. Cˇ apkun. Jamming-resistant broadcast communication without using shared keys, in procedings of the USENIX Security Symposium, 2009.
[4] Anti-jamming broadcast communication usng uncoordinated frequency hopping, P.Manjula, S. Sharmila, Assistant Professor, Veltech Multitech Engineering College,International journal of Innovation in engineering and management(IJAIEM), June 2013.
[5] Fast rendezvous for cognitive radios by exploiting power leakage at Adjacent Channels, Li Zhang, Kefeng Tan, Kai Zeng, Prasant Mohapatra, PIMRC, 2012.
[6] On the Capacity of Rate-Adaptive Packetized Wireless Communication Links under Jamming, Koorosh Firouzbakht, Guevara Noubir, Masoud Salehi, WISEC, 2012.
[7] Analysis and Study of Denial of Service Attacks in Wireless Mobile Jammers, S.M.K Chaitanya1, P. Naga Raju, Y.N.V.L. Ayyappa, Vundavalli Ravindra, IJCST, 2011.
[8] FPGA based wireless networks, N. Radha krishnaiah, Mrs.P.Brunadevi, IJMER, 2013.
[9] Passive Diagnosis for Wireless sensor networks, Yunhao liu, Kebin Liu, Mo li, IEEE, 2010.
[10] Keyless Jam Resistance, Leemon C. Baird III, William L.Bahn, Michael D. Collins, Martin C. Carlisle, Sean C, Butler,IEEE, 2007.

