ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 10, October 2016

Frequency Hopping and Rate Adaptation Based Time Delayed Broadcast Scheme to Overcome Jamming Attacks

M.Priyanga[1], C.Vinola[2], B.Benita[3]

PG Student, Department of CSE, Francis Xavier Engineering College, Tirunelveli, India[1]

Assistant Professor, Department of CSE, Francis Xavier Engineering College, Tirunelveli, India[2]

Assistant Professor, Department of CSE, Francis Xavier Engineering College, Tirunelveli, India[3]

ABSTRACT: The broadcast type of wireless communications leaves them vulnerable to various security threats, including jamming attacks. Adversaries can use easily available off-the-shelf commercial products to launch stealth jamming attacks. In literature, Frequency Hopping (FH) and Rate Adaptation (RA) have been separately used to mitigate jamming. When RA is used only, it has been shown that jammers who chance its power levels can force the transmitter to always operate at the minimum rate, by continuing the average jamming power above a certain threshold. On the other hand, when only FH is used, a maximum throughput overhead was brought upon yourself due to frequent channel switching. Here Time-Delayed Broadcast Scheme (TDBS) with a combination of Frequency Hopping Spread Spectrum (FHSS) and Rate Adaptation is introduced. Each node is assigned FH sequence with unique values. TDBS implements the broadcast operation as a series of unicast transmissions distributed in frequency and time. TDBS is specifically designed to facilitate broadcasting in dynamic broadcast groups by constructing rainbow paths in theproperedge- colored graphs. TDBS with FH and RA does not rely on commonly shared secrets or the presence of jamming-immune control channels for coordinating broadcasts. This way, the transmitter can escape from the jammer by changing its channel, adjusting its rate, or both. Thus the security control and time delay reduction are achieved through RSA algorithm and Time Delayed Broadcast Scheme in awireless network.

KEYWORDS: Broadcast communications, FHSS, Jamming attacks, Security, wireless sensor networks

I. INTRODUCTION

Network security is defined by the protection of networks and their services from unauthorized users. Network security contains the authorization of access to data in a network, which is controlled by the network administrator. Users are assigned an ID and password or other verifying information that allows them access to information and programs within their authority. Network security contains a variety of computer networks, both public and private, that are used in everyday jobs; handling transactions and communications among businesses, government agencies, and individuals. Aparticular company using the network private, and others which might be open to public access. Network security is involvedin organizations, enterprises, and other variety of institutions.It secures the network, as well as protecting and inspecting the operations being done. The most common and easy way of protecting a network resource is by assigning it a unique name and a corresponding password.

Wireless communications are vulnerable to premeditated interference attacks, typically referred to as jamming.Conventional anti-jamming techniques depend on spread spectra (SS) communications, such as a direct sequence spread spectrum (DSSS) and frequency hopping spread spectrum (FHSS)[6].DSSS provides bit-level protection by spreading bits according to a secret pseudorandom noise (PN) code, well- known only to the communicating parties. In FHSS, the sender and the receiver hop synchronously using a secret random frequency [7][11].

The jamming attack is one of the most demanding security issues in wireless networks, which disseminates out sufficient adversaries radio frequencies used by normal sensor nodes, without following any legitimate protocols. Since the jammer obstructs with radio reception by producing noise, it could decrease the probability of successful broadcasting in the wireless communication [12]. The jammers do not need to examine lots of internal information of the network components, so this lightweight attack is easy to launch and favored by attackers. Furthermore, in reactive jamming attacks [8], the jammers have idle until being triggered by messages disseminated within their transmission ranges, thereby further decreasing the jammers operation overhead and making it hard to detect. Thus this intelligent attack could be utilized by malicious users in more real-world scenarios.

Their existing system [1], the methodused Uncoordinated DSSS (UDSSS),in which broadcast transmissions are spread according to a PN codearbitrary, selected from a public codebook [10]. Receivers decode transmitted messages by exhaustively implementing every PN code in the public codebook. The main disadvantages of theexisting systemare a dependency on shared secrets and in most PHY-layer standards.Frame detection is based on the signal cross-correlation between the received signal and thewell-known preamble and does not require preamble decoding.

The Time-Delayed Broadcast Scheme (TDBS) has beenintroduced as an emergency mechanism for temporarily restoring broadcast communications until inside jammers are physically detached from the network.TDBS differs from classical FHSS designs in that two communicating nodes do not consecutive the same FH sequence, but assign unique values. TDBS is specifically designed to expedite, broadcasting in the presence of jammers and the series of unicast distributed in frequency and time. TDBS is specifically designed to helpto broadcast in the presence of jammers [9] in the absence of a coordinated channel. The problemhasbeen updatesof the FH sequences of existing nodes when the broadcast groups are changing.This problem is mapped to the structure of a rainbow path of fixed size in proper edge-colored complete graphs. Note that TDBS is not represented as a permanent replacement of the conventional broadcast mechanism. Broadcasting on a common frequency band accomplishes the optimal communication efficiency in the absence of any jammer.TDBS is designed as an emergency mechanism for momentary restoring communications until the jammer is physically removed.

II. RELATED WORK

In [2] Pelechrinis K., Koufogiannakis C., and Krishnamurthy S. V. discussed on the efficacy of frequency hopping in coping with jamming attacks in 802.11 networks. The objective of this work is to understand the interactions between a jammer and a communication link and to evaluate the efficacy of frequency hopping in coping with jamming attacks. The main focus is on proactivefrequency hopping strategies for both the communication and the jamming. The reactive jamming case is more complicated. The efficacy of a reactive jammer is affected by a number of factors. The measurement-based game theoretic framework technique is used to capture the intercommunication between a link and a jammer employing proactive FH.To apply our framework, all these parameters need to be accurately modeled and measured. Using this way, increase the transmission rate and when only FH is used, a high throughput overhead was brought upon yourself due to frequent channel switching.In [3] Popper C., Strasser M., and Capkun S. discussed Anti-jamming broadcast communication using uncoordinated spread spectrum techniques, Spread spectrum techniques use data-independent, arbitrary sequences to spread a narrowband information signal over a wide (radio) band of frequencies. The proposed Uncoordinated Spread Spectrum(USS) techniques that implement anti-jamming communicationbetween sender and receivers that do not share any secretkeys. Thus the implementation is used to create a solution of the problem with anti-jamming broadcast and anti-jamming key establishment. USS techniques accomplish this by removing the requirement of pre-shared secrets at the expense of a reduced communication delay and also increased the storage overhead.In [4] Firouzbakht K., Noubir G., and Salehi M. introduce on the capacity of rate-adaptive packetized wireless communication links under jamming. Rate adaptation plays an important role in widely used wireless communication systems. The problem of resolving the optimal rate control and adaptation mechanisms for a channel subject to a power strained jammer. A setup is considered where a pair of nodes communicates using data packets.An adversary can interfere with the communication but is strained by an instantaneous maximum power per packet (J_{Max}) and a long-run average power (J_{Ave}). Appropriately coded packets can overcome interference and are lost otherwise. Over-coding reduces the throughput, while under-coding increases the chances of losing a packet.In [5]Zhang Y., Li Q., Yu G., and Wang B. introduce ETCH, efficient channel hopping based communication rendezvous protocols for Dynamic Spectrum Access(DSA) networks. DSA is a promising

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 10, October 2016

technique that solves the spectrum scarcity problem and raises network capacity. In DSA networks, unlicensed users are granted the right of accessing licensed spectrum while the licensed users are not using them.ETCH, Efficient Channel Hopping based MAC-layer protocol is proposed for a communication rendezvous in DSA networks. ETCH protocols include SYNC-ETCH and ASYNC-ETCH. A combination of theoretical analysis and simulations is efficiently utilized the frequency diversity in establishing control channels for DSA network nodes for a communication rendezvous in DSA networks. Thus the implementation leads to a high probability of traffic collision and low traffic throughput in DSA network.

III. **PROPOSED TDBS SCHEMEIN MULTI-HOP NETWORKS**

A. *OVERVIEW OF TDBS:*

To achieve jamming-resistant communications in the existence of insiders, TDBS implements broadcast as a series of unicasts distributed in frequency and time. The locations of these unicast, defined by a frequency band/ slot pair (f, s), are only partially known to each node. Therefore, a compromised node announces only the set of locations assigned to it, while the locations of other communications are kept secret. For this purpose, nodes are isolated into pairs scheduled to communicate over randomly selected frequency bands. The pairs and assigned frequency bands varied on a per-slot basis, thus realizing an FH system. TDBS differs from traditional FH designs in that,

- Nodes do not follow a common, FH sequence, but hop according to unique hopping patterns
- These patterns are coordinated to reduce the broadcast delay.

TDBS can operate in two modes. They are Sequential Unicast mode (SU) and Assisted Broadcast mode (AB).

TDBS-SU: Sequential Unicast mode

The sender sequentially relays information to intended receivers. This more inefficient mode is not trusted to relay broadcast messages.

TDBS-AB: Assisted Broadcast Mode

In the AB mode, any node that has already received a broadcast message operates as a broadcast relay.

B. *SYSTEM MODEL AND SECURITY:*

The broadcast operation of TDBS scheme is extendedin multi-hop networks.The FH sequence design can be viewed as a global scheduling problem. While several distributed methods have been proposed in distributed scheduling [13], [14].Using these methods requires coordination via a common channel. However, such a channel can be blocked by an inside jammer. So to create a scalable solution that does not rely on the existence of a common channel. The trusted Central Authority (CA) partition the network into clusters where each cluster forms a clique.The broadcast operation is divided into two phases; an intra-cluster phase and an inter-cluster phase. During the intra-cluster phase, communication is limited within each cluster. In the inter-cluster phase, messages are exchanged between border nodes of adjacent clusters. The two phases are interleaved in time.

Fig 1 describes that for every node deployment starts before the CA check that the user is a trusted user or not. Based on the security parameter the trusted user is decided. Every user has a specific private/public key value. The CA is distributing private/public key pair in sender to the receiver with the help of RSA algorithm. If the only trusted user is allowed to access the network others are moved to the warning list.For every node v_i, the CA generates a public/private key pair <pki; ski>. Node v_i is preloaded with the CA’s public key pk CA and its own secret key ski.To communicate message m to vi, the CA encrypts mjjsni with pki and signs ðidijjmjjsniÞ with its private key <sk> CA. Here, id is vi’s unique, sni is a random sequence number that is incremented by one with every message sent to v_i, and jj denotes message concatenation.

DOI: 10.15680/IJIRCCE.2016. 0410022

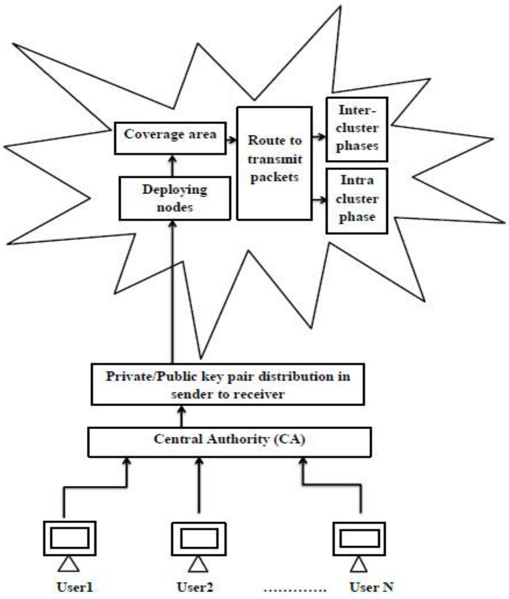

Fig 1. System Architecture

Algorithm 1: RSA Algorithm
Step 1: A public and private key are created on the server (CA).

Step 2:When theuserhit a web server, the web server sends the public key<pki> to the appropriate user.
PublicKey=EncryptPrime+ProductOfPrime1Prime2

Step 3: Web server are never sent the PrivateKey<ski>.
PrivateKey=DecryptPrime+ProductOfPrime1Prime2

Step 4: This works because theuser cannot evolve Encrypt Prime from Decrypt Prime and ProductOfPrime1Prime2.User encrypts everything, the usersends to the web server with the Public Key and they encrypt everything they send to theweb server with the Private Key.

Step 5: User can decrypt what the server sends me, but alone the server can decrypt what they send back. So when user type in your Password into at your blank web page, your password is sent encrypted so only the server can decrypt it.

The security of the data during aggregation is ensured. By achieving this security, the central authority is provided by each user. The central authority checks whether the user is an authorized user or attacker. The accessing permission is only provided to the authorized user.

C.*CHANNEL ALLOCATING FOR CLUSTERING SENSOR NETWORK:*

Authorized users are deploying the nodes in a random manner. Each node forms a cluster and each cluster has a leader, which is also called the cluster head (CH) and usually performs the special taskassigned above (fusion and aggregation) and several common sensor nodes (SN) as members. The cluster formation process eventually advantages to a two-level hierarchy where the CH nodes form the highest level and the clustermember nodes form the lower level. The sensor nodes regularly transmit their data to the corresponding CH nodes. The broadcast group is dynamic.

Specifically, to design a node addition mechanism that minimizes the changes in the FH schedule of existing nodes by constructing rainbow paths in complete graphs. These techniques are used to communicatethe modified FH schedule with existing nodes using the newly deployed node, without adirect connection to the CA.For node deletion mechanism, the remaining nodes are modified from their original FH schedule to an optimal schedule for 2n- 2 nodes.This modification is performed individually, without any information exchange. The dynamic broadcast operation is divided into two phases.

Inter-cluster phase

In the inter-cluster phase, border nodes relay broadcast messages beyond the origin cluster. To do so while avoiding scheduling conflicts, we exploit the cluster coloring produced by the four-color theorem. During this phase, every time slot is marked with one of the four colors, indicating the clusters that are allowed to transmit on that slot.

Theorem 1:Four-colorTheorem

Step 1:For each cluster x,find the nodes in x bordering adjacent clusters. Place these nodes to a set A.

Step 2: For each v_i Ɛ A, find the neighbors of vi in adjacent clusters and assign them to vi. If a neighbor is common to more than one node in x, assign it to the node with the fewer neighbors. Break ties arbitrarily. Merge nodes assigned to the same v_i to a single vertex and place vertices to set B. Create a bipartite graph G(A U B, Ɛ). Where an edge(v_i, v_j) exists if nodes corresponding to v_jƐ B are assigned to v_i Ɛ A. By construction, graph G forms a 1-factor Fx.

Step 3: For each slot colored with x's color, obtain a random permutation π Ɛ P_K.

Step 4: Assign frequency bands in p to the first min{n, K} unassigned pairs of Fx:

Step 5: Repeat Steps 3 and 4 until all pairs in Fx are assigned a frequency band.

Step 6: Repeat Steps 1–5, until all clusters are processed.

Intra-cluster phase

In the intra-cluster phase, a broadcast message propagates to all cluster nodes. Because the nodes of a cluster form a clique, the SU or the AB mode of TDBS can be employed for broadcast. To avoid interference between adjacent clusters, the set of available frequency bands C is partitioned into four subsets, which are assigned to clusters according to the four-color theorem.

Theorem 2: Four-color Theorem

Step 1: Color each cluster using the four-color theorem.

Step 2: Assign a subset of channels to each cluster according to its color.

Step 3: For each cluster, construct FH sequences using either the SU mode or the AB mode.

IV.SIMULATION RESULT

Fig 2 represents the amount of data transmitted from one place to another or processed in a specified amount of time. Data transfer rates for disk drives and networks are calculated in terms of throughput. Typically, throughputs are calculated in kbps, Mbps and Gbps.The data are transmitted in a secure manner, therefore, increasing through.Fig 3 represents the End-to-end delay or one-way delay (OWD) to the time taken for a packet to be transmitted across a network from source to destination. It is a natural term in IP network monitoring and differs from Round-Trip Time (RTT).The performance analysis of delay time is performed between the number of data/packets and the delay time.

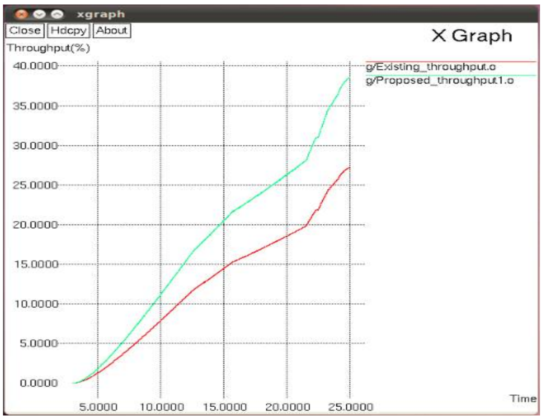

Fig 2: Comparison between time vs throughput

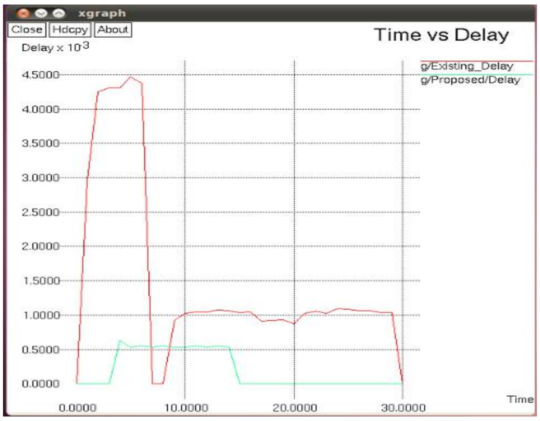

Fig 3: Comparison between time vs delay

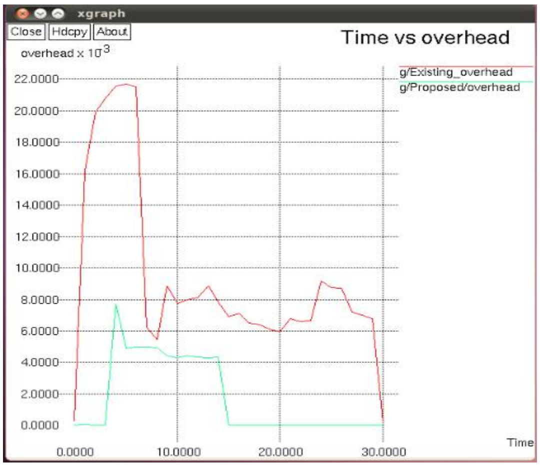

Fig 4: comparison between time vs overhead

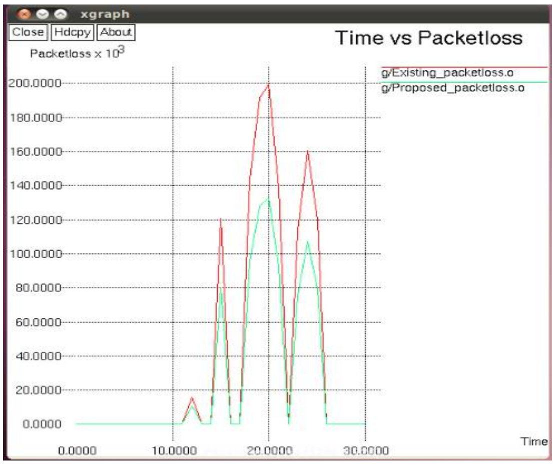

Fig 5: Comparison between time vs packet loss

In Fig 4, the graph is plotted between the overhead of the packets and the time.In Fig 5 represents the packet loss between the existing and proposed system. The data are transmitted in a secure manner, therefore, decreasing packet loss.

V.CONCLUSION

TDBS is a scheme to overcome the jamming attacks for broadcast communications in the presence of inside jammers. TDBS implements the broadcast operation is realized as a series of unicast transmissions distributed in frequency and time. It is specifically designed to facilitate broadcasting in dynamic broadcast groups by constructing rainbow paths in proper edge-colored graphs. The transmitter can use this scheme to maintain broadcast communications, even when multiple nodes are compromised. Here TDBS with a combination of FHSS and RA is introduced. But each node is assigned FH sequence with unique values. This way time delay reduction is achieved by constructing dynamic broadcast group for communication since verification has been done by the Central Authority. Thus the implementation is helpful to achieve the collision-free channel allocation and increase security control and throughput and also avoid packet loss in thewireless network.

REFERENCES

1. Sisi Liu, Loukas Lazos,"Time-Delayed Broadcasting for Defeating Inside Jammers", IEEE Transaction on dependable and secure computing, vol.12,may/June 2015.
2. Pelechrinis. K, Koufogiannakis. C, and Krishnamurthy. S. V,"On the efficacy of frequency hopping in coping with jamming attacks in 802.11 networks", IEEE Transactions on Wireless Communications, vol. 9, no. 10, pp. 3258–3271, October 2010.
3. C. Popper, M. Strasser, and S. Capkun, "Anti-jamming broadcast communication using uncoordinated spread spectrum techniques," IEEE J. Sel. Areas Commun., vol. 28, no. 5, pp. 703–715, Jun. 2010.
4. Firouzbakht. K, Noubir. G, and Salehi. M, "On the capacity of rate-adaptive packetized wireless communication links under jamming", in Proc. of the ACM WiSec Conf., Tucson, AZ, USA, 2012, pp. 3–14.
5. Zhang. Y, Li. Q, Yu. G, and Wang. B, "ETCH: Efficient channel hopping for communication rendezvous in dynamic spectrum access networks", in Proc. INFOCOM Conf., 2011, pp. 2471–2479.
6. Zhang. Y, Yu. G, Li. Q,Wang. H, Zhu. X, and Wang. B, "Channel hopping-based communication rendezvous in cognitive radio networks", IEEE/ACM Trans. Netw., vol. 22, no. 3, pp. 889–902,Jun. 2014.
7. Liu. S, Lazos. L and Krunz. M (2011), "Thwarting inside jamming attacks on wireless broadcast communications", in Proc. 4th ACM WiSec Conf., pp. 29–40.
8. Yilin Shen, Ying Xuan, and Thai. T, "Reactive Jamming Attacks in Multi-Radio Wireless Sensor Networks: An Efficient Mitigating Measure by Identifying Trigger Nodes", ACM 978-1-60558-523-9/09/05, May 2009, New Orleans, Louisiana, USA.
9. Bian. K, Park. J and Chen. R (2009), "A quorum-based framework for establishing control channels in dynamic spectrum access networks", in Proc. MOBICOM Conf., pp. 25–36.
10. Y. Liu, P. Ning, H. Dai, and A. Liu, "Randomized differential DSSS: Jamming-resistant wireless broadcast communication", in Proc. INFOCOM Conf., 2010, pp. 1–9.
11. Baird. L. C, Bahn. W. L,Collins. M. D, Carlisle. M. Cand Butler. S. C (2009), "Keyless jam resistance", in Proc. IEEE Workshop Inf. Assurance United States Military Acad.
12. Popper. C, Strasser. M, and Capkun. S, "Jamming-resistant broadcast communication without shared keys", in Proc. USENIX Security Symp., 2009, pp. 231–248.
13. Chaporkar. P, Kar. K, Luo. X, and Sarkar. S, "Throughput and fairness guarantees through maximal scheduling in wireless networks," IEEE Trans. Inf. Theory, vol. 54, no. 2, pp. 572–594, Feb.2008
14. Gupta. ALin. X, and Srikant. R, "Low-complexity distributed scheduling algorithms for wireless networks", IEEE/ACM Trans. Netw., vol. 17, no. 6, pp. 1846–1859, Dec. 2009.