Overcome Jamming Attacks using TDBS with Compromise Resilient Anti-Jamming Scheme in WSN

M. Priyanga*, S. Malaiarasan, B. Benita
Department of CSE, Francis Xavier Engineering College, Tamil Nadu, India
***Corresponding author: E-Mail: priya29392m@gmail.com**

ABSTRACT

The broadcast type of wireless communications leaves them vulnerable to various security threats, including jamming attacks. Attackers can use easily available bought commercial products to launch stealth jamming attacks. The Frequency Hopping Spread Spectrum and Rate Adaptation was combined and achieved in the existing system. The unique frequency value is assigned to all nodes in the network. It is specifically designed to promote broadcasting in dynamic broadcast groups by making rainbow paths in the proper edge- colored graphs. These processes with combined FH and RA. Secrets cannot be shared among them. However, it could be accessible to insider jammers and leakage of information to hackers. The present system will be scheme called compromise-resilient anti-jamming or split-pairing. The network will execute and distribute a new group key. It will be shared all compromised nodes and increase the maximum signal strength only by insider jammer happening nodes. Thereafter, it will be unable to predict the future communication channels used by compromised nodes because the insider jammer is revoked. Using this method, the transmitter can easily escape from the inside jammer by changing its channel, adjusting its rate, or both. Thus the security control and time delay reduction are achieved through Group Key Establishment algorithm and present scheme in a wireless network.

KEY WORDS: Broadcast Communications, Jamming attacks, Security, Wireless sensor networks.

1. INTRODUCTION

Wireless communications are vulnerable to premeditated interference attacks, usually referred to as jamming. 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, and not for other legitimate protocols.

The jammers are no use to examine lots of internal information of the network components, so this lightweight attack is easy to launch and favored by attackers. In future, the reactive jamming attacks, the jammers have idle thereby further decreasing the jammers operation overhead and to create it hard to detect.

Their existing system method with a combination of frequency value and rate was implemented. Each node is assigned frequency sequence with unique values. It is specifically designed to perform a broadcast process in dynamic broadcast groups to making the rainbow paths in the proper edge- colored graphs. Secrets cannot be shared using these methods. However, it could be accessible to insider jammers and leakage of information to hackers.

The proposed system will be scheme called compromise-resilient anti-jamming or split-pairing. The network will create a new group key. This key will be shared all compromised nodes and increase the maximum signal strength only by insider jammer happening nodes. Thereafter all the future communication channels will be unable to predict. Then used by compromised nodes because the insider jammer is revoked. Using this way, the transmitter can easily escape from the inside jammer by changing its channel, adjusting its rate, or both. Thus the security control and time delay reduction are achieved through group Key Establishment algorithm and current methods in a wireless network.

Related Work: Firouzbakht (2012), introduced the capacity of rate adaptive is an important technique. It is mostly used wireless communication systems. The problem of resolving the optimal value control and adaptation mechanisms for a channel subject to a power strained jammer. A setup is considered as two nodes communicate 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 decreases the throughput and under-coding increases the chances of losing a packet.

Pelechrinis (2010), discussed work is in between a jammer and a communication link and to evaluate the strength of the signal in jamming attacks. It focuses on proactive frequency hopping action for both the communication and the jamming. The reactive jamming case is more complicated. The measurement-based framework technique is used to adsorb the intercommunication between a link and a jammer employing proactive TD. To apply our framework, all these parameters used to be accurately modeled and measured. Using this way, increase the transmission rate and when only SD is used, a high throughput overhead was brought upon yourself due to frequent channel switching.

Popper (2010), discussed the spread spectrum techniques use data-independent, arbitrary ranges of strengths to spread according to them. The proposed techniques that implement anti-jamming communication between sender and receivers that do not share any secret keys. Thus the implementation is needed to create a solution of the problem with anti-jamming communication and anti-jamming key establishment. USS techniques accomplish this by eliminating the requirement of pre-shared secrets at the expense of a reduced communication delay and also increased the storage overhead.

Sisi Liu and Loukas Lazos (2015), have proposed the Uncoordinated DSSS broadcast transmissions are spread in PN code arbitrary, preferred from a public codebook. Receivers decode messages by thoroughly implement the public codebook. The main disadvantage of the existing system is shared secrets dependency. Frame detection can follow the signal cross-correlation between the received signal and the well-known preamble and does not need preamble decoding.

Zhang (2011), introduce the technique is a hopeful technique. That solves the spectrum scarcity problem and raises network capacity. In the networks, unlicensed users have accepted the right of accessing licensed spectrum and correct users are not using them. These protocols include SYNC-ETCH and ASYNC-ETCH. It is efficiently utilized the frequency diversity in establishing control channels for network nodes for a communication among the dynamic networks. Thus the implementation top to a high probability of traffic collision and low traffic throughput in the network.

2. PROPOSED METHOD WITH SPLIT-PAIRING SCHEME IN MULTI-HOP NETWORKS

Overview of TDBS: To achieve jamming-resistant communications in the already present in insiders, it implements broadcast and unicast transmission to distribute the frequency and time in a serial manner. The place of these nodes frequency band/ slot pair (f, s), are only partially known to each node. Therefore, a corrupted node announces only the set of locations assigned to it, while the positions of other communications are kept secret. It is very helpful the nodes are isolated into pairs scheduled to communicate over randomly selected frequency bands. The assigned frequency bands varied on a per-slot basis, thus realizing a frequency system. It varies from traditional frequency hop and network designs in that,

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

TDBS is operating in two modes. They are,

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

System model and security: It is the existing method is extended in multi-hop networks. The design can be shown the global scheduling problem. The several distributed scheme was proposed in distributed scheduling. 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 and that not share the data's in common channel. The trusted Authority partition the network into clusters where each cluster forms a clique.

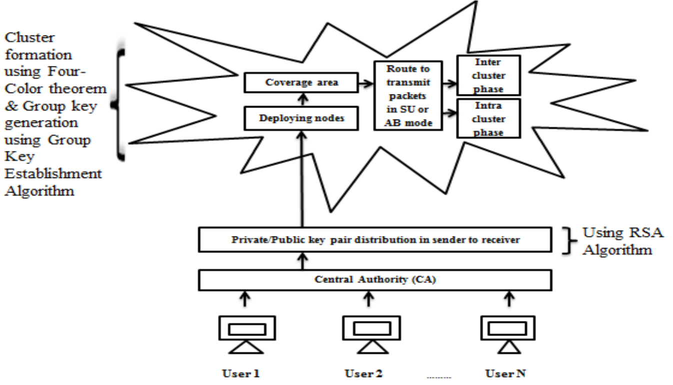
Cluster formation using Four-Color theorem & Group key generation using Group Key Establishment Algorithm
Coverage area
Deploying nodes
Route to transmit packets in SU or AB mode
Inter cluster phase
Intra cluster phase
Private/Public key pair distribution in sender to receiver
Using RSA Algorithm
Central Authority (CA)
User 1
User 2
User N

Figure.1. Proposed System Architecture

The broadcast transmission is classified into two phases; an intra-cluster phase and an inter-cluster phase. The intra-cluster phase, communication is limited within each cluster. In the inter-cluster phase, information's are interchanged 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 customer is a trusted user or not. With help of the security parameter the trusted user is decided. Every man has a specific private/public key value.

The authorized party is distributing private/public key pair in sender to the receiver with the help of RSA algorithm. If the only trusted men are allowed to access the network others are moved to the warning list. For every node v_i, it generates a public/private key pair <pk_i; sk_i>. Node v_i is preloaded with the trusted member's public key pk and its own secret key sk_i. To communicate message m to v_i, the authorized user encrypts mjjsni with pk_i and signs $id_j jmjjsn_i$ with its private key <sk>. Here, id is v_i's unique, sn_i is a random sequence number that is incremented by one with every message sent to v_i, and jj denotes message concatenation.

Algorithm 1: RSA Algorithm:

Step 1: The security keys are created on the network.

Step 2: When the user hit a web server, and to sends the public key<pk_i> to the appropriate user.

Public Key=Encrypt Prime + Product of Prime1 Prime2

Step 3: Web server are never sent the Private Key<sk_i>.

Private Key=Decrypt Prime + Product of Prime1 Prime2

Step 4: This works because the user cannot evolve Encrypt Prime from Decrypt Prime and Product of Prime1 Prime2. User encrypts everything, the user sends the Public Key and they encrypt everything they send to the Internet the Private Key.

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

The security of the data during aggregation is ensured. By achieving this security, the central authority is provided by each user. They check real user or attacker. The accessing permission is only provided to the authorized person.

Channel Allocating for Clustering Sensor Network: Authorized users are deploying the nodes not in a uniform manner. Each node forms a cluster and all cluster groups have one leader, which is also called the cluster head and many common sensor nodes as members. The cluster allocation has a two-level. The CH nodes are the highest level and the cluster member nodes are the lower level. The sensor nodes regularly transmit their data to the corresponding head nodes. The broadcast group is dynamic. Specifically, to design a node addition mechanism in the frequency range schedule of existing nodes by developing the rainbow paths in complete graphs.

Compromise-Resilient anti-Jamming scheme in Clustering Sensor Network: The cluster formation process has been done. After each cluster group can generate a common key with the help of Group Key Establishment algorithm. Using this way, to establish a common key between the authorized persons of a group, without disclosing it to other parties. The original member protocols are also addressed as qualified, legitimate or privileged. A protocol runs for multiple times, named sessions.

Each meeting is exceptionally recognized by a session id, which can be computed during the performance of the protocol or given in advance by the environment. The insider jamming arrives at the time. The network is immediately generating a new group key to be shared only by all compromised nodes. The insider jammer is revoked and it will be used for the future communication channels. Instead, each node follows a different pseudo-noise frequency hopping ranges of the sequence are kHz, MHz, and GHz. The broadcasting is categorized into two phases.

Inter-cluster phase: In the inter-cluster phase, edge 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, referring the clusters that are allowed to transmit on that slot.

Theorem 1: Four-color Theorem:

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

Step 2: For each v_i Ɛ A, find the nears of v_i in adjacent clusters and assign them to v_j. If a neighbor is common at most 1 node in x, assign it to the node with the fewer neighbors. Break ties arbitrarily. Merge nodes assigned to the same v_i in 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_j Ɛ B are assigned to v_i Ɛ A. By construction, graph G forms a 1-factor Fx.

Step 3: Each slot colored with x's color and the 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 & 4 until all pairs in F_x are specified a frequency band.

Step 6: Repeat Steps 1 to 5. Then all clusters are processed.

Intra-cluster phase: In the intra-cluster phase, a broadcast message transferred to all cluster nodes. Because the nodes of a cluster form a unique, these two modes of the scheme can be employed for broadcast. They avoid distrust between adjacent clusters, the pair 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: Each cluster using the four-color theorem.

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

Step 3: For each cluster, construct frequency hop sequences using either the unicast mode or the broadcast mode.

3. SIMULATION RESULT

Performance analysis: Fig.2, represents the amount of data processed in a specified amount of time. Data transmission rates for disk drives and networks are calculated in terms of throughput. Typically, throughputs are calculated in Kbps, Mbps, and Gbps. The data are passed in a secure manner, therefore, increasing throughput.

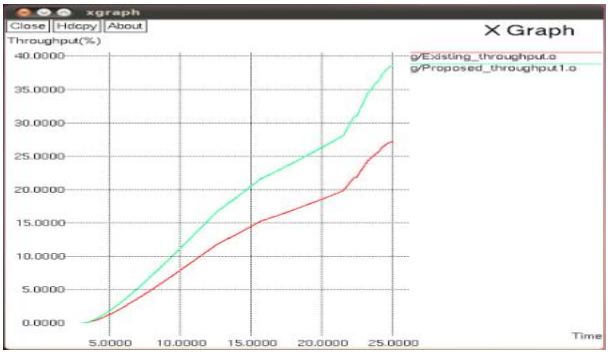

Figure.2. Comparison between time vs throughput

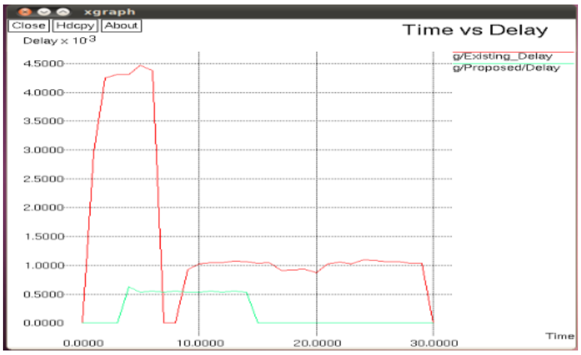

Figure.3. Comparison between time vs delay

Fig.3, represents the End-to-end delay to the time taken for a packet to be sent across a network from sender to receiver. The delay time is performed between the number of data/packets and the delay time.

4. CONCLUSION

The time delay broadcast method with the compromise-resilient anti-jamming is involved and to overcome the jamming attacks for broadcast communications in the present of internal jammers. With the use of these techniques to control the key leakage of a subset of sequences by compromised nodes and to maintain broadcast communications, the multiple nodes are compromised. This way time delay is reduced for this communication since verification has been done by the Trusted Central Authority. Thus the implementation is helpful to remove inside jammers and increase security control and throughput and also avoid damages in a wireless network.

REFERENCES

Baird L.C, Bahn W.L, Collins M.D, Carlisle M.C and Butler S.C, Keyless jam resistance, in Proc. IEEE Workshop Inf. Assurance United States Military Acad., 5, 2009, 1873-1888.

Chaporkar P, Kar K, Luo X and Sarkar S, Throughput and fairness guarantees through maximal scheduling in wireless networks, IEEE Trans. Inf. Theory, 54 (2), 2008, 572–594.

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, 3–14.

Liu Y, Ning P, Dai H and Liu, A Randomized differential DSSS, Jamming-resistant wireless broadcast communication, in Proc. INFOCOM Conf, 8, 2010, 1–9.

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, 9 (10), 2010, 3258–3271.

Popper C, Strasser M and Capkun S, Anti-jamming broadcast communication using uncoordinated spread spectrum techniques, IEEE J. Sel. Areas Commun., 28 (5), 2010, 703–715.

Popper C, Strasser M and Capkun S, Jamming-resistant broadcast communication without shared keys, in Proc. USENIX Security Symp, 11, 2009, 231–248.

Priyanga M, Vinola C and Benita B, Frequency Hopping and Rate Adaptation Based Time Delayed Broadcast Scheme to Overcome Jamming Attacks, International Journal of Innovative Research in Computer and Communication Engineering, 4 (10), 2016, 17232-17238.

Sisi Liu, Loukas Lazos, Time-Delayed Broadcasting for Defeating inside Jammers, IEEE Transaction on dependable and secure computing, 12, 2015.

Yilin Shen, Ying Xuan and Thai T, Reactive Jamming Attacks in Multi-Radio Wireless Sensor Networks, ACM New Orleans, Louisiana, USA, 2009.

Zhang Y, Li Q, Yu G and Wang B, ETCH, Efficient channel hopping for communication rendezvous in dynamic spectrum access networks, INFOCOM Conf., 2011, 2471–2479.

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., 22 (3), 2014, 889–902.