A Security Mechanism Against Reactive Jammer Attack In Wireless Sensor Networks Using Trigger Identification Service

Ramya Shivanagu[1] and Deepti C[2]

[1]PG Student, The Oxford College of Engineering, India
ramya.shivanagu@gmail.com
[2]Asst Professor, The Oxford College of Engineering, India
deeptic82@gmail.com

ABSTRACT

Providing an efficient security for wireless sensor network is a crucial challenge which is made more difficult due to its broadcast nature and restrictions on resources such as energy, power memory usage, computation and communication capabilities. The Reactive Jammer Attack is a major security threat to wireless sensor networks because reactive jammer attack is a light weight attack which is easy to launch but difficult to detect .This work suggest a new scheme to neutralize malicious reactive jammer nodes by changing the characteristic of trigger nodes to act as only receiver. Here the current approach attempts to identify the trigger nodes using the group testing technique, which enhances the identification speed and reduces the message complexity of the status report sent periodically between the sensor nodes and the base station.

KEYWORDS

Wireless sensor network, Jamming Techniques, Reactive jamming, Trigger identification.

1. INTRODUCTION

Wireless sensor networks has limited resource constraints in terms of energy and range which leads to many challenging and intriguing security-sensitive problems that cannot be handled using conventional security solutions. The broadcast nature of the transmission medium makes it prone to attacks using jammers which use the method of injecting interference signals, which is why they can be considered as the most critical and fatally adversarial threat that can disrupt the networks. Jamming attacks do not have to modify communication packets or compromise any sensors in order to launch the attack.This makes them difficult to detect and defend against. As a consequence, wireless sensor networks are further exposed to passive and active attacks. A malicious node initiates a passive attack [1] through inert observation of the ongoing communication, whereas an active attacker is involved in transmission as well.

1.1. Jamming Techniques

The spot jamming technique [2] involves a malicious node that directs all its transmitting power to a single frequency. It makes use of identical modulation schemes and less power to override the original signal. The assault on WSNs due to this attack is easily avoided by surfing to another

DOI : 10.5121/ijsptm.2013.2204

frequency. In case of Sweep jamming technique [3], the malicious node can jam multiple communication frequencies, but this jamming does not affect all the involved nodes simultaneously. The attack also leads to packet loss and retransmission of packet data that will increase consumption of energy in the network.

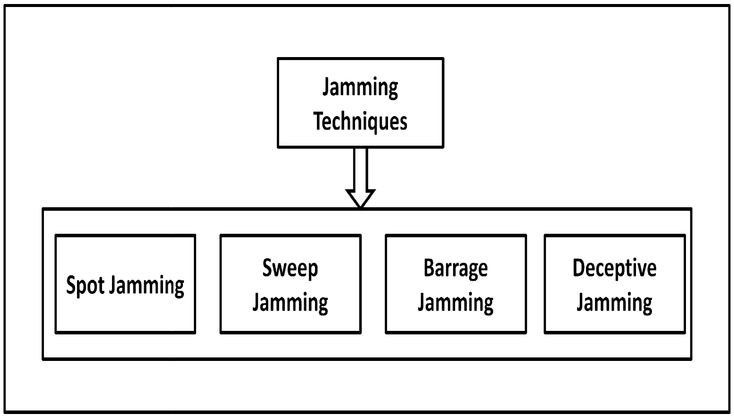


Fig 1: Different types of jamming techniques

Figure 1 is an illustration of the types of jamming techniques used in general to launch jammer attacks. In Barrage jamming technique[4], the malicious node jams a group of frequencies simultaneously which decreases the signal-to-noise ratio of the destination node. This jamming technique increases the range of jammed frequencies and reduces the output power of the jammed node. Deceptive jamming[5] has the capability to flood the network with useless data which can mislead the sensor nodes present in the network .The available bandwidth used by the sensor nodes is reduced. The malicious nodes that make use of this technique do not reveal their existence.

1.2. Jamming Types

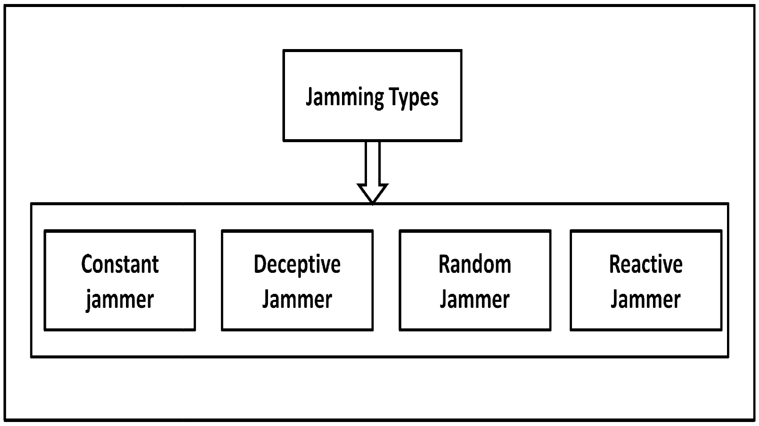


Fig 2: Types of jammers

Figure 2 depicts several types of jammers that may be used in attacks against wireless sensor networks namely constant jammer, deceptive jammer ,random jammer and reactive jammer. The constant jammer [6] emits uninterrupted radio signals in the wireless medium. They do not follow any underlying MAC protocol and include just random bits. This jammer keeps the channel busy

and disturbs the communication between the nodes. The deceptive jammer [7] uses misleading jamming techniques to attack the wireless sensor nodes. The random jammer [8] sleeps for an indiscriminate time and wakes up to jam the network for an arbitrary time. The last jamming approach indicated above is the reactive jammer [9] which listens for on-going activity on the channel. On detection of legitimate activity, the jammer node immediately sends out a random signal to disrupt the valid communication signals prevalent on the channel leading to collision.

1.3. System Architecture

The inference after comparing the above mentioned jamming attacks is that reactive jamming is a far more destructive attack that opposes secure communication in wireless sensor network. This paper considers the reactive jammer attack since it poses a critical threat to wireless sensor networks as the reactive jammer nodes can disrupt the message delivery of its neighbouring sensor nodes with strong interference signals. The consequences of the attack are the loss of link reliability, increased energy consumption, extended packet delays, and disruption of end-to-end routes.

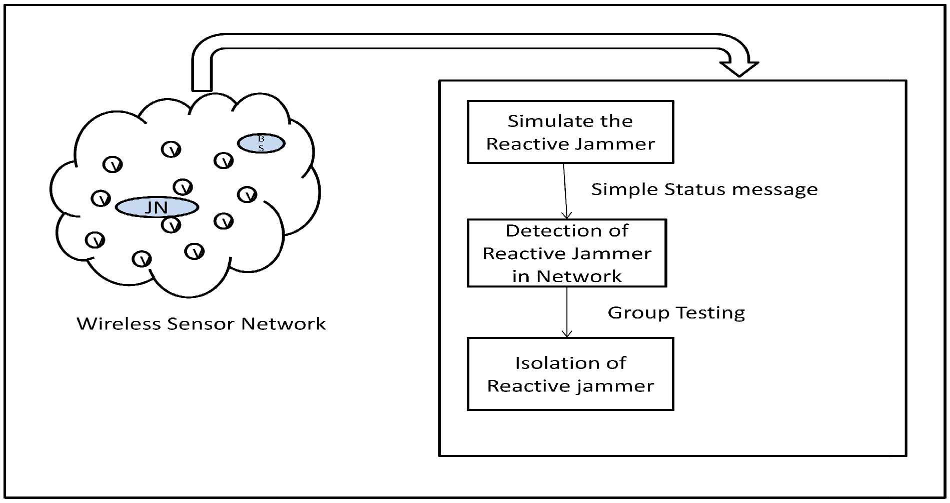

B
S
JN
Wireless Sensor Network
Simulate the Reactive Jammer
Simple Status message
Detection of Reactive Jammer in Network
Group Testing
Isolation of Reactive jammer

Fig 3: System Architecture

This work presents system architecture for defense against reactive jamming attack. The initial description of the overall trigger identification service framework begins with the identification of the set of sufferer nodes .These nodes are then grouped into several testing teams. Once the group testing is carried out at the base station, the nodes themselves locally execute the testing procedure to identify each individual node as a trigger or non trigger. The identification outcomes can be stored locally for use by routing schemes or can be sent to the base station for jamming localization process. The rest of the work is organized as follows. Section 2 explains the network model, and the attacker model along with jamming characteristics. Section 3 describes the implementation approach for trigger identification service by making use of group testing. Section 4 describes the performance evaluation by analysis of the time complexity involved along with evaluation of the time taken to execute the testing rounds and also the message complexity.

2. SYSTEM MODELS AND NOTATION

2.1. Network Model

The model considers a wireless sensor network that consists of n sensor nodes and one base station. Each sensor node has omni-directional antennas, along with m radios that adds up to a total of k channels throughout the network, where k>m. Here the power strength in each direction is considered to be uniform, so the transmission range of each sensor can be considered as a constant r and the network is modelled as a unit disk graph (UDG). where any node pair (i , j) is said to be connected if the Euclidean distance between (i, j) < r.

2.2. Attacker model

The jammer nodes can sense an ongoing transmission to decide whether or not to launch a jamming signal depending on the power of the sensed signal. The assumption made here is that reactive jammers have omnidirectional antennas with uniform power strength on each direction which is similar to the property of the sensors. The jammed area created by the reactive jammers lies on the centre of the network area, with a radius R, where jammer range R is required to be greater than the range of all the sensors in the network in order to achieve a powerful and efficient jammer model. All the sensors within this range will be jammed during the jammer wake-up period. The value of R can be calculated based on the positions of the boundary sensors and victim nodes in the networks. Another assumption is that any two jammer nodes are not in close range with each other so as to maximize the jammed area.

2.3. Sensor model

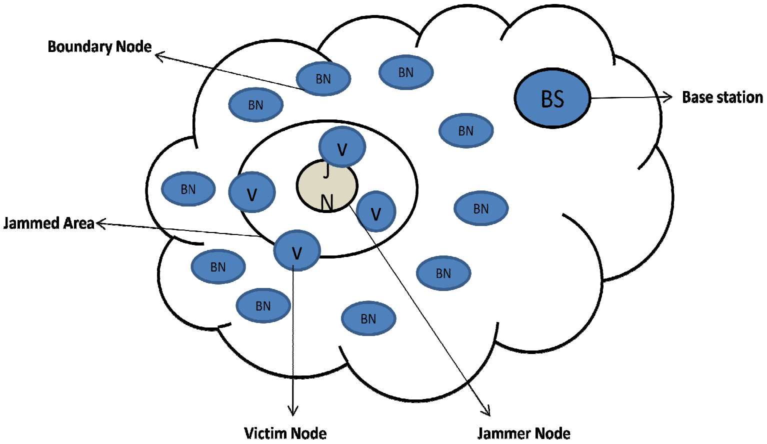


Fig 3: Categorization of Sensor Nodes

The jamming status is utilised to categorise the sensor nodes into four types as shown in Figure 3.Trigger Node TN is a sensor node which awakes the jammers, victim nodes VN are those within a distance R from an activated jammer, boundary nodes BN and unaffected nodes are free from the effect of jammers.

3. IMPLEMENTATION APPROACH USING TRIGGER IDENTIFICATION

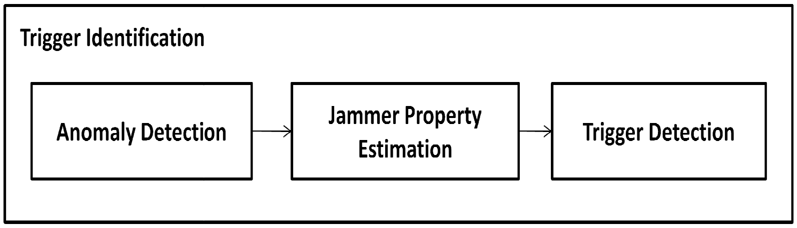
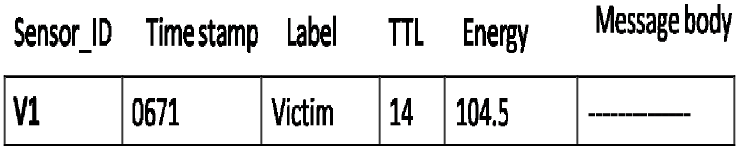


Fig 4: Trigger identification procedure

Trigger identification service is mainly divided into three main steps as shown in Figure 4. The first step executes anomaly detection where the base station detects impending reactive jamming attacks. Each boundary node identifies itself to the base station. In the second step jammer property estimation is performed where the base station calculates the estimated jammed area and jamming range based on the location of boundary node. The third step is trigger detection where the base station broadcasts a short testing schedule message M to all the boundary nodes .Thereafter the boundary nodes keep broadcasting M to all the victim nodes within the estimated jammed area for a period P.Subsequently the victim nodes locally execute the testing procedure based on M and identify themselves as trigger or nontrigger.

The non-adaptive Group Testing (GT) method can be used to minimize the testing period by sophisticatedly grouping and testing the items in pools simultaneously, instead of individually testing them. This way of grouping is based on a 0-1 matrix Mt×n where the matrix rows represent the testing group and each column refers to an item. M[i , j] = 1 implies that the j^{th} item participates in the ith testing group, and the number of testing is the number of rows. The result of each group is represented as an outcome vector with size t where 0 is a negative testing result (no trigger in this testing group) and 1 is a positive result (possible triggers in the testing group). To achieve the minimum testing length for non-adaptive GT, M is required to be d-disjunct, where the union of any d columns does not contain any other column.

Step 1: Anomaly Detection



Sensor_ID	Timestamp	Label	TTL	Energy	Message body
V1	0671	Victim	14	104.5	----------

Fig 5: Status report message

Figure 5 shows the status report message having four tuples: Source_ID gives the ID of the sensor nodes, Time stamp indicates the sequence number, Label gives present jamming status, TTL field indicates packet transmission time and energy.

In anomaly detection every sensor periodically sends a status report message to the base station. There is a possibility that jammers may be activated during this period .This occurrence will not allow report messages from the compromised sensors to be received by the base station. The base station can decide whether jamming attack has occurred in the network or not by comparing the ratio of received report to a predefined threshold.

Step 2: Jammer Property Estimation

The jammed area and jamming range D will be calculated by the base station by considering the location of boundary and victim nodes. In this work sparse-jamming is considered where the distribution of jammers is relatively sparse and there is no overlap between the jammer nodes. By denoting the set of boundary nodes for the ith jammed area as $BN_{i,}$ the jammer coordinate can be estimated as

$$(Xj,Yj)=\{\ \sum_{k=1}^{BNi}\frac{Xi}{BNi},\sum_{k=1}^{BNi}\frac{Yk}{BNk}\ \} \qquad (1)[20]$$

Where (X_k ,Y_k) is the coordinate of a node k is the jammed area BN_i and jamming range D is

$$D=\min\{\max(\ \sqrt{}(Xk-Xj)^2+(Yk-Yj)^2)\} \qquad (2)[20]$$

Step 3:. Trigger Detection

The jammers immediately broadcast jamming signals once it senses the ongoing transmission by the sensors. The jammers are identified by trigger identification service. Here encrypted testing schedule is adhered by all the victim nodes. Scheduling will be done at the base station based on the set of boundary nodes and the global topology. Information with regard to topology is stored as a message and broadcast to all boundary nodes. After receiving the test scheduling message, each boundary node broadcasts the message by using simple flooding method to its adjoining jammed area. All victim nodes implement the testing schedule and specify themselves as trigger or non-trigger node.

```
Algorithm :Trigger Nodes Identification Algorithm

/*All nodes in a group N synchronously performs the following to recognize trigger nodes in N.*/
INPUT: n victim nodes in a testing group
OUTPUT: all trigger nodes within these victim nodes

//In order to estimate d i.e. upper bound of error
Set $\gamma=(10t- 8t^2 - t^{-d} -1)/2$;

//Likelihood for each test
Set $T=t \ln n(d+1)^2/(t- \sqrt{(d+1)})^2$;

Construct a (d,z)- disjunct matrix using ETG algorithm with T rows, and divide all the n victim nodes into T group accordingly {g1,g2,.....,gt};

// Group testing will be done for each round on m groups using m  different channels. Here testing can be done in asynchronous manner ,the m group tested in parallel  need  not wait for each other to finish the testing, instead any finished test j will trigger the test j+m, i.e,  the tests are conducted in m pipelines.

for i= 1 to [t/m] do

    Conduct group testing in group gim+1,gim+2,gim+m in parallel;
    If any node in group gj with j€ [im+1,im+m] detects jamming noises, finish the testing in this group and start testing on gj+m;
    If  no nodes in group gj sense jamming noises, while at least one other test in parallel detects jamming noises,
        All the nodes in group gj resend  more messages to set off possible hidden jammers;
    If  no jamming signals are detected till the end of the predefined round length (L)
        Return a negative outcome for this group and start testing on gj+m;

End
```

As shown in algorithm above, the groups can decide to conduct group testing on themselves in m pipelines. If any jamming signals occur in pipeline ,then the current test will be stopped and the next test has to be scheduled. The groups receiving no jamming signals are required to resend triggering messages and wait until the predefined round time has passed.

4. PERFORMANCE EVALUATION AND RESULT ANALYSIS

The results of these experiments show that this solution is time efficient for identifying trigger nodes and defending reactive jamming attacks. The trigger identification procedure for reactive jamming in network simulator NS2[21] on 900×900 square sensor field with n=10 sensor nodes has been simulated. The sensor nodes are uniformly distributed, with one base station and J distributed jammer nodes. In this work ,the sensor transmission radius r and jamming transmission R as 2r has been considered to achieve better efficiency of the jamming model.

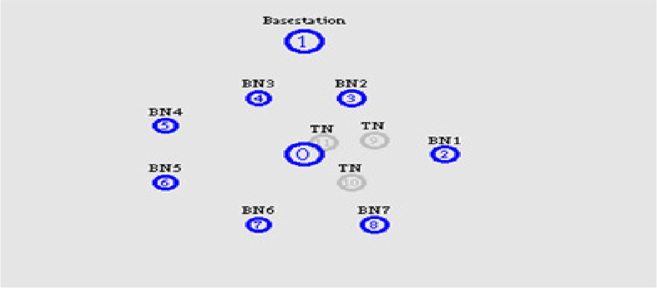


Fig 6: Simulation of reactive jamming

Figure6 shows a network simulated with 10 sensor node with 1 malicious node and 1 base station. The transmission range(r) of ordinary sensor node is set as 50m while jammer transmission range(R) set to 100m(2r).

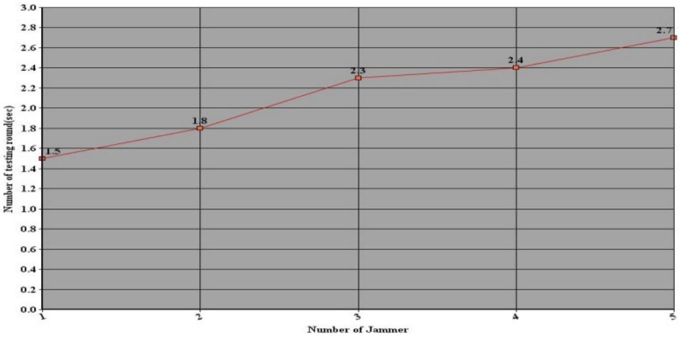


Fig 7: The number of testing rounds t(sec)

Figure7 explains the protocol performance based on the variation in the numbers of jammers J in the network. In this test,N = 10 nodes with m = 3 radios, on a 900×900 network field have been considered where J ∈ [1, 5] jammers are uniformly deployed. Group testing employs a sophisticated technique to perform as many parallel tests as possible so that the estimated number of testing rounds T(sec) can be stable even though the number of jammers J increase.

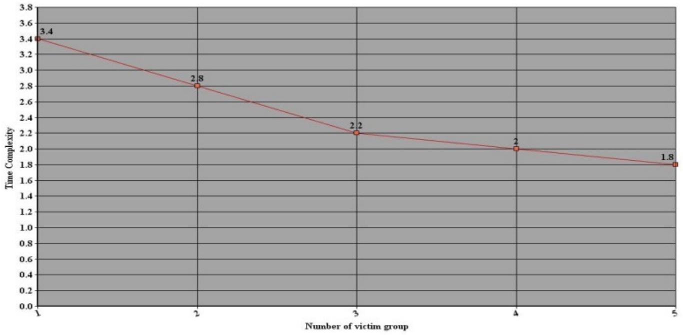


Fig 8: Time Complexity.

In order to show that the trigger identification service for reactive jamming attack is more efficient, group testing has been performed on different groups simultaneously for detecting the trigger node. With this reduction in time complexity can be demonstrated.Figure8 shows that time complexity can be reduced as the number of victim nodes that execute testing procedure in the group increase.

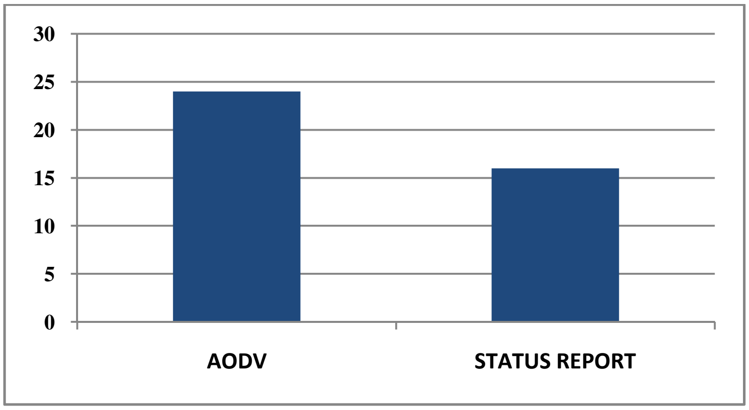


Fig 9: Message Complexity.

This work considers simple status message transfers between the sensor node and base station that can provide reduction in message complexity as compared to AODV(Ad hoc On-Demand Distance Vector) which makes use of unnecessary bandwidth consumption due to periodic beaconing that leads to message overhead. Figure9 shows that message complexity is reduced in the case of implementation of the trigger identification service.

5. RELATED WORK

One of the reactive countermeasures uses Adapted Breadth-First Search Tree algorithm for identification of jammer node[13]. Here the base station broadcasts a message to all n nodes along a BFS tree. Once a node receives this message, it will set its corresponding entry to one. If the node senses that any one of the channels is jammed, another normal channel is used to transmit the broadcast message. The base station will receive a collection of messages from all leaf nodes. In this case, the number of ACKs from the leaf nodes leads to overhead in base station.

Another approach for the detection and mapping of jammed area [14] has been proposed by Wood and Stankovic to increase network efficiency. However, this method has several drawbacks: first, it cannot practically defend in the situation that the attacker jams the entire network; second, in case the attacker targets some specific nodes i.e. those that guard a security entrance to obstruct their data transmission, then this technique fails to protect the nodes under attack.

Xu [15] proposed two strategies against jammers i.e, channel surfing and spatial retreat. Channel surfing is adaptive form of FHSS. Instead of switching continuously from one channel to another, a node switches to a channel only when it discovers that the current channel is free from jammer. The spatial retreat method makes two nodes to move in diverse ways with separation atleast equal to Manhattan distances [16] to get away from a jammed region. The disadvantages of the above mentioned methods are that they are valuable only for constant jammers and they have no effect on reactive jamming.

The concept of Wormhole [17] can be used to bypass the jammed areas which disturb the regular communication of the sensor nodes. These solutions can only effectively reduce the intensity of the jamming attacks, but their performance depends on the accuracy of detection of the jammed areas, i.e. transmission overhead would be needlessly involved if the jammed area is much larger than its actual size. Victim nodes cannot efficiently avoid jamming signals because they do not possess knowledge over possible positions of hidden reactive jammer nodes, especially in dense sensor networks

This paper proposes a fresh implementation move towards defence of the network against reactive jamming attack i.e. trigger identification service [18-19]. This can be considered as a lightweight mechanism because all the calculations are done at the base station. This approach attempts to reduce the transmission overhead as well as the time complexity. The advantage that this approach seeks to achieve is the elimination of additional hardware requirement. The requirement of the mechanism is to send simple status report messages from each sensor and the information regarding the geographic locations of all sensors maintained at the base station.

6. CONCLUSION

In this paper, a novel trigger identification service for reactive jamming attack in wireless sensor network is introduced to achieve minimum time and message overhead. The status report message are transferred between the base station and all sensor nodes . For isolating reactive jammer in the network a trigger identification service is introduced, which requires all testing groups to schedule the trigger node detection algorithm using group testing after anomaly detection. By identifying the trigger nodes in the network, reactive jammers can be eliminated by making trigger nodes as only receivers. This detection scheme is thus well-suited for the protection of the sensor network against the reactive jammer. Furthermore, investigation into more stealthy and energy efficient jamming models with simulations indicates robustness of the present proposed scheme. The result can be stored in the network for further operations i.e. to perform best routing operation without jamming. This work achieves the elimination of attackers to maintain the soundness of wireless sensor networks.

REFERENCES

[1] G. Padmavathi,“A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks,” vol. 4, no. 1, pp. 1–9, 2009.

[2] LV Bo,ZHANG Xiao-fa,WANG Chao ,YUAN Nai-chang," Study of Channelized Noise Frequency-spot Jamming Techniques",2008

[3] XI You-you,CHENG Nai-ping**,** **"**Performance Analysis of Multi-tone Frequency Sweeping Jamming for Direct Sequence Spread Spectrum Systems",2011.

[4] Williams united state ," Multi-Directional Barrage Jamming System",1975.

[5] J. Schuerger, "Deceptive Jamming Modelling In Radar Sensor Networks,” pp.1–7.

[6] W. Xu et al., “Channel Surfing and Spatial Retreats: Defenses Against Wireless Denial of Service,” Proc. 2004 ACM Wksp. Wireless Security, 2004, pp. 80–89.

[7] W. Xu et al., “The Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks,” MobiHoc ’05: Proc. 6th ACM Int’l. Symp. Mobile Ad Hoc Net. and Comp., 2005, pp. 46–57.

6] W. Xu et al., “Channel Surfing and Spatial Retreats: Defenses Against Wireless Denial of Service,” Proc. 2004 ACM Wksp. Wireless Security, 2004, pp. 80–89.

[7] W. Xu et al., “The Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks,” MobiHoc ’05: Proc. 6th ACM Int’l. Symp. Mobile Ad Hoc Net. and Comp., 2005, pp. 46–57.

[8] Y. Law et al., “Link-Layer Jamming Attacks on S-Mac,” Proc. 2nd Euro. Wksp. Wireless Sensor Networks, 2005, pp. 217–25.

[9] A. Wood and J. Stankovic, “Denial of Service in Sensor Networks,” IEEE Comp., vol. 35, no. 10, Oct. 2002, pp. 54–62.

[10] D. Report, C. Science, and J. Bacaj, “Detecting Attacks in Wireless Sensor Networks,” 2011.

[11] A. Mpitziopoulos, D. Gavalas, C. Konstantopoulos, and G. Pantziou, “A survey on jamming attacks and countermeasures in WSNs,” *IEEE Communications Surveys & Tutorials*, vol. 11, no. 4, pp. 42–56, 2009.

[12] M. Wilhelm, I. Martinovic, J. B. Schmitt, and V. Lenders, “Short Paper : Reactive Jamming in Wireless Networks — How Realistic is the Threat ? PHY packet,” pp. 0–5, 2011.

[13] W. Xu, W. Trappe, Y. Zhang, T. Wood, \The Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks", in Proc. of the 6th ACM international symposium on Mobile ad hoc networking and computing, pp. 46-57, 2005.

[14] C. Gao, X. Hu, L. Guo, W. Xiong, and H. Gao, "A Data Dissemination Algorithm using Multi-Replication in Wireless Sensor Networks," no. 1, pp. 91–93, 2013.

[15] W. Xu, W. Trappe, and Y. Zhang, "Channel Surfing: Defending Wireless Sensor Networks from Interference," *2007 6th International Symposium on Information Processing in Sensor Networks*, pp. 499–508, Apr. 2007.

[16] N. P. Nguyen and M. T. Thai, "A Trigger Identification Service for Defending Reactive Jammers in WSN," *IEEE Transactions on Mobile Computing*, vol. 11, no. 5, pp. 793–806, May 2012.

[17] M. Cagalj,S.Capkun, and J. P. Hubaux. "Wormhole- Based Antijamming Techniques in Sensor Networks."IEEE Transactions on Mobile Computing,2007.

[18] I. Shin, Y. Shen, and Y. Xuan, "Reactive Jamming Attacks in Multi-Radio Wireless Sensor Networks : An Efficient Mitigating Measure by Identifying Trigger Nodes," pp. 87–96, 2009.

[19] Y. Xuan,Y. Shen, I. Shin, and M.T. Thai, "A Graph-theoretic Framework for Identifying Trigger Nodes against," vol. 6, no. 1, pp. 1–14, 2007.

[20] R. Niedermeier and P. Sanders,"On the Manhattan-Distance between the points on Space-fillinh mesh Indexing", pp. 1–10, 1996.

[21] T. V. Project, U. C. Berkeley, X. Parc, K. Fall, and E. K. Varadhan, "The ns Manual (formerly ns Notes and Documentation) 1," no. 3, 2009.

[22] A. D. Wood, J. Stankovic, and S. Son. "A jammed-area mapping service for sensor networks. " *RTSS '03*, pages 286–297, 2003.

Authors

Miss Ramya Shivanagu received her Bachelor of Engineering in Information Science and engineering in 2010. Currently She is a M.Tech student in Computer Networking Engineering from Visvesvaraya Technological University at The Oxford College of Engineering, Bangalore. Her research interests are wireless sensor networks, Network Security.

Mrs Deepti C received her Bachelor of Engineering in Electronics and Communication in 2004. She received her M.Tech in Computer Network Engineering with distinction from Visvesvaraya Technological University in 2009. Currently she also holds a faculty position as Assistant Professor, Department of ISE, The Oxford College of Engineering. Her main research interests are signal processing, wireless sensor networks, wireless network security .