Jamming Detection System in Wireless Sensor Networks

K.P.Vijayakumar, P.Ganeshkumar, M.Anandaraj

Abstract—**Jammers may easily attack the Wireless Sensor Networks. Hence it is essential for securing these networks from malicious nodes. In this paper, a novel system is proposed to detect the node's maliciousness level for securing WSN's from jamming attacks in cluster-based sensor network. The proposed System that detect the maliciousness level using Packet Delivery Ratio. First, it protects the network from those external nodes that are already announced as jammers. Secondly, it detects those nodes that are being becoming an adversary. The simulation result demonstrates that the proposed system detects the maliciousness level extremely well and achieves high jammer detection rate and low false detection rate**

Index Terms—**malicious level, jamming attack, packet delivery system, jammer detection rate, false detection rate**

I. INTRODUCTION

Wireless sensor networks consists of many sensor nodes which sense the physical conditions like temperature, pressure and sound etc,. A sensor node consists of memory, communication device, power supply, sensors and actuators. This paper focus on Clustering-based sensor networks. A cluster consists of Cluster Head (CH) and Cluster Members (CMs). Cluster Heads communicate via Base station (BS) and Cluster members communicate through cluster head.

Jammer prevents the successful communication between source and destination. Jammer node is a node which prevents the signal transmission between two nodes. There are two types of jammer nodes. They are internal jammer nodes and external jammer nodes. Internal jammer nodes are defined as the node that is present in the cluster has a chance to become jammer in future. External jammer nodes are defined as the nodes that are present outside the clusters. There are four types of jammer [3]. They are: Constant jammer, Deceptive jammer, Random jammer and Reactive jammer. Constant Jammer is the emission of random bits which keeps the channel busy and finally the packets will be collided. Deceptive Jammer is a dangerous type of attack through which the attacker does not show their presence. It misleads WSN's operator to provide fake data. Random jammer switches between constant jammer and deceptive jammer. Reactive jammer listens for the channel activity and collide the packets finally. Apart from this type of jamming there are also additional jammers like Spot jammer, Barrage jammer, Sweep jammer [4]. The primary motivation for our study is,

- **Node centric to network centric**: The proposed method, CHs compute and process the PDR to make decision about jammed condition or not jammed condition.
- **Reduces communication overhead:** The proposed approach, individual node doesn't communicate with CH in making decision.

The rest of the paper is organized as follows. Section 2 involves the related works. Section 3 explains the system model. Section 4 consists of simulation results. Section 5 consists of conclusion and future work.

II. RELATED WORKS

Aristides [3] proposed the concept of Denial of Service (DoS). It demonstrates the jamming issue of WSN. Jamming is just an undesirable noise and is effective if SNR<1. Some of the security schemes like detection techniques, proactive and reactive countermeasures against jamming in WSN is also proposed. Sudip Misra[1] explained the concept of different possible metrics for jamming detection. The metrics for jamming attack detection like Carrier Sensing Time (CST), Packet Delivery Ratio (PDR), Packet Sent Ratio (PSR), Bit Error Rate (BER) and Bad Packet Ratio (BPR). The author selected metrics for his paper are SNR and BPR. Tran Van Phuong [5]proposed the concept of anomaly detection in WSN for detecting attacks like wormhole attacks, HELLO attacks, Collision, etc., An algorithm for anomaly detection is being proposed i.e. CUSUM algorithm. He proposed that it's a strongest of all algorithms. A threshold is being set for the anomaly detection. Wenyuan et al [9] proposed the concept of jamming attacks and defense strategies into two approaches. They are (i) to retreat from the interferer. (ii) to achieve the communication by adjusting resources such as power levels and communication coding.

Mario Stresser[7] proposed the concept of detection of reactive jammers. A novel jamming detection scheme is being proposed to identify the bit error causes based on the received signal strength. This identification can be done in three ways as pre-determined knowledge, error correcting codes and limited wiring. Rajani muraleedharan [6] shows the jamming attacks and its countermeasures in wireless sensor networks in ant system. The author proposed DoS attack analysis and defense mechanism is proposed. He

K.P.Vijayakumar, Department of IT, PSNA College of Engineering and Technology, Tamil Nadu, Dindigul.
P.Ganeshkumar,. Department o IT, PSNA College of Engineering and Technology, Tamil Nadu, Dindigul.
M.Anandaraj. Department of IT, PSNA College of Engineering and Technology, Tamil Nadu.

stated four types of jammers such as single-tone jammer, Multi-tone jammer, Pulsed-noise jammer and ELINT. Idris et al [2] proposed the concept of malicious node detection using weighted trust evaluation. It consists of three nodes such as sensor nodes, Forwarding nodes and Base Station. A weight is being assigned for each sensor nodes and a threshold is set so that the weight must be lower than the threshold value, then it is a malicious node. [8] Yu Sueng kim proposed the concept of localizing a wireless node by two steps. They are (i) the jammer's location is being discovered (ii) the localization protocol is also discovered.

III. SYSTEM MODEL

There are two Cluster Heads referred as CH1 and CH2 can communicate via the Base Station (BS) as shown in Fig.1. Members M1 and M2 are present in the cluster 1 and members M3 and M4 are present in the cluster 2. Each member can communicate with others through CH. The jammer node jams the nodes 1 and 4. We assume that the coverage area is application-dependent. Jamming will take place within its coverage area of the jammer.

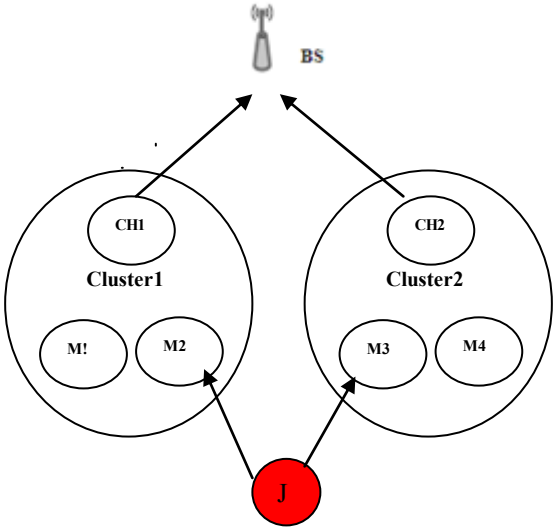

Fig. 1: System Model

IV. PROPOSED SYSTEM

The proposed work consists of two functionalities. First, it performs an authentication that whether the node is legitimate node or jamming node. To achieve this, it uses two tables namely Member Table and Jammer Table as shown in Table I and Table II. Member table includes Member Id and type of a node. Type denotes about type of the node like Base Station or Cluster Member. The Jammer Table includes Node Id. Next, PDR_Monitor(), which monitors the member's behavior to detect the malicious level of cluster members.

If a CH receives a packet then it checks with the Member table and Jammer table to verify that the node is legitimate member or jammer node. If Id of the node is matched with the Member Id in both the tables then it is declared as jammer node. Otherwise it is a new node. Data flow of the authentication is shown in the Fig. 2. Algorithm1 explains the principle of authentication.

Algorithm1: Authentication

Input: Node Id or Member Id
Output: Performs normal task or discard it

```
Begin
Packet Receive
If (Node.Id== Member.Member.Id)
    If (Node.Id == Jammer.MemberId)
       Then
          Declare Node as Jammer node
          Discard the packet
       Else
           Perform normal task
           PDR_Monitor()
    End if
 Else
       If (Node.Id !=  Jammer.MemberId)
           Then
              Declare as New Node
              Perform normal task
              PDR_Monitor ()
        End if
End If
End
```

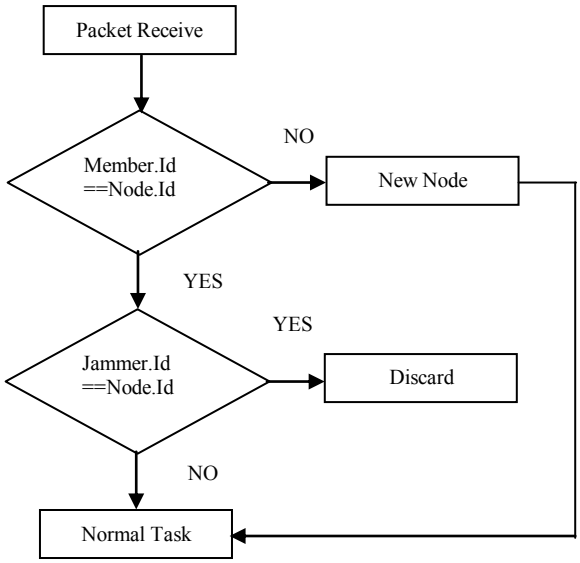

Fig. 2. Data Flow Diagram for authentication

TABLE: I MEMBER TABLE

Member Id	Type
M1	M
M2	M
B1	B

TABLE: II JAMMER TABLE

Member Id
M2
M3

Two clusters 1 and 2 consisting of members namely M1, M2 and M3, M4 respectively. Member table consist of three entries where M1 and M2 denotes cluster members and B1 represents Base Station as shown in Table1. The PDR_Monitor() algorithm monitors the cluster member's behavior to detect the maliciousness level as shown in Algorithm2.

Algorithm: PDR_Monitor ()
Input: Cluster members
Output: Malicious Level
Threshold_value=75%
Begin
  Receive data packets
  Check reception of Ack
  If (Ack is received)
    Status is S
  Else
    Status is U
  End If
  Update Status Table
  Compute PDR of every Cluster Members
  For i=1 to N (N is number of CH)
    For j=1 to M (M is number of CM)
      Select Max_PDR of CMj
      If Max_PDR > Threshold_value
        M_level is High
      Else If Max_PDR == Threshold_value
        M_level is Normal
      Else
        M_level is Low
      End If
    End For
  End For
End

Once the node is declared as legitimate node or new node then algorithm 2 in invoked. If the CH receives the acknowledgment from its corresponding members, then the CH updates the Status table as either U or S. After that, every CH, computes the PDR of its members. Then it determines the maliciousness level as shown in the Table III.

TABLE: III MALICIOUS LEVEL TABLE

S.No.	Member Id	M_level
1	M1	Low
2	M2	High
3	M3	High
4	M4	Low

Algorithm 3 shows that the CH computes the PDR of its members using the Status table. , the status table's member.id is checked with the member id of Member Table. If the status is S then the PDR_D is incremented. Otherwise, the PDR_UD is incremented. PDR [4] is the ratio of PDR_D to the PDR-UD. The value updated in the PDR Table using the below given formula, The PDR table is updated at each 100sec as shown in the Table IV.

$$pdr = pdr\_d / pdr\_d + pdr\_ud \qquad (1)$$

TABLE IV. PDR TABLE

S.No.	Member Id	PDR
1	M1	100
2	M2	62
3	M3	55
4	M4	99

Algorithm 3: PDR computation
Input: Member Table, Status Table
Output: PDR Table
Begin
  Time_int: 100 sec.
  For i =1 to N
    For j=1 to M
      For k= 1 to P (P is total no. of record)
        Fetch k^{th} record from status table
        If (Status.Member Id ==Member.MemberId)
          If(Status.status=='S')
            PDR_D=PDR_D+1;
          Else
            PDR_UD=PDR_UD+1;
          End If
        End If
      End For
  End For
End

V. SIMULATION RESULT

The simulation is done using NS2 simulator for detection of maliciousness level for group of nodes**.** The values of PDR and Max_PDR are simulated. Fig. 3shows the malicious level for the group of nodes. Fig. 4 shows the true detection ratio for various types of configurations. Fig.5 shows the false detection ratio for various types of configuration.

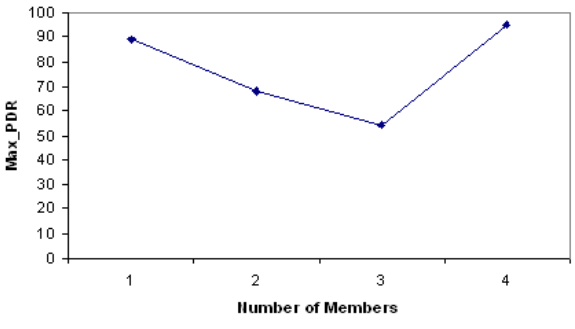

Fig.3 Represents Number of nodes and Max_PDR

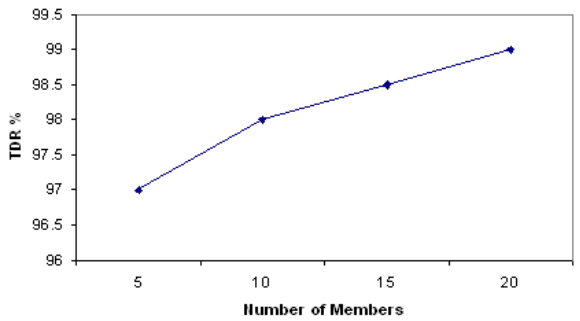

Fig. 4 Represents true detection ratio of various member configurations

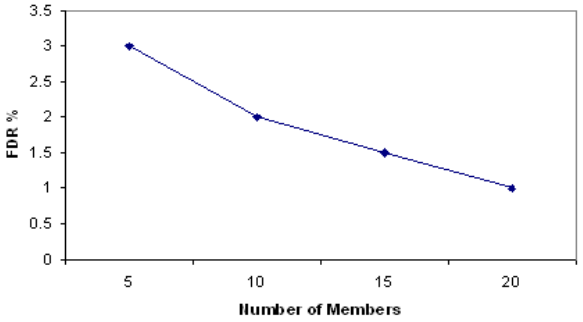

Fig.5 Represents false detection ratio of various member configurations

VI. CONCLUSION

We first discussed different types of jamming and various jamming detection techniques. The proposed system works as, authenticate that the node is legitimate node or jammer node and then monitor the behavior of members to detect the maliciousness level of cluster members. The packet delivery ratio selected as metric for determining the maliciousness level of nodes. A threshold value 75%) is set to determine the maliciousness level of the jammer. The simulation results shows us to achieve the high jammer detection rate and low false detection rate.

In our proposed work, we need an authentication scheme to verify that the new node existed in other cluster during mobility.

REFERENCES

[1] Sudip Misra 1, Ranjit Singh and S. V. Rohith Mohan. "Information Warfare-Worthy Jamming Attack Detection Mechanism for Wireless Sensor Networks Using a Fuzzy" ISSN 1424-8220. Published: 8 April 2010 Sensors , 3444-3479;

[2] Idris M. Atakli, Hongbing Hu, Yu Chen SUNY – Binghamton Binghamton "Malicious Node Detection in Wireless Sensor Networks using Weighted Trust Evaluation", NY 13902, USA, submitted on Jan. 11, 2008 to The Symposium on Simulation of Systems Security (SSSS'08), Ottawa, Canada, April 14 –17,08.

[3] Aristides Mpitziopoulos, Damianos Gavalas, Charalampos Konstantopoulos, and Grammati Pantziou. "A Survey on Jamming Attacks and Countermeasures in WSNs", IEEE communications surveys & tutorials, vol. 11, no. 4, fourth quarter 2009.

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

[5] Tran Van Phuong, Le Xuan Hung, Seong Jin Cho, Young-Koo Lee and Sungyoung Lee."An Anomaly Detection Algorithm for Detecting Attacks in Wireless Sensor Networks" Computer Engineering Dept. Kyung Hee University 449-701 Suwon, Republic of Korea.

[6] Rajani Muraleedharan and Lisa Ann Osadciw "Jamming Attack Detection and Countermeasures In Wireless Sensor Network Using Ant System" Department of Electrical Engineering and Computer ScienceSyracuse University Syracuse, NY 13244-1240.M. Young, *The Techincal Writers Handbook.* Mill Valley, CA: University Science, 1989.

[7] Mario strasser, boris danev, and srdjan cˇ apkuneth Zurich "Detection of Reactive Jamming in Sensor Networks", Switzerland ACM Transactions on Sensor Networks, Vol. 7, No. 2, Article 16, Publication date: August 2010 .

[8] Yu Seung Kim, Frank Mokaya, Eric Chen, and Patrick Tague "All Your Jammers Belong To Us - Localization of Wireless Sensors Under Jamming Attack"Electrical and Computer EngineeringCarnegie Mellon University Moffett Field, CA 94035-0001.

[9] Wenyuan Xu, Ke Ma, Wade Trappe, and Yanyong Zhang "Jamming Sensor Networks:Attack and Defense Strategies" Rutgers University IEEE Network May/June 2006

K.P.Vijayakumar received his B.E. degree in Information Technology from Madurai Kamaraj University (India) in 2003, his M.E. degree in Computer Science and Engineering from Anna University Chennai (India) in 2007, and doing Ph.D. degree in Information and Communication Engineering at Anna University, Chennai. He has been working as an Associate Professor in the Department of Information Technology at PSNA College of Engineering and Technology, India since June 2003. His research interests include computer networks, network optimization, Wireless network, ADHOC Network, network security.

P. Ganeshkumar is a Professor in the Department of Information Technology at PSNA College of Engineering and Technology, India since December 2002. He received his B.E degree in Electrical and Electronic Engineering from Madurai Kamaraj University , India in 2001, his M.E. degree in Computer Science and Engineering from the Bharathiyar University (India), and his Ph.D. in Information and Communication Engineering at Anna University, Chennai. His research interests include AdHoc Network, Wireless Networks, and Distributed Systems.

M.Anandaraj received his B.E. degree in Computer Science and Engineering from Madurai Kamaraj University (India) in 2003, his M.E. degree in Computer and Communication from Anna University Chennai (India) in 2007, and doing Ph.D. degree in Information and Communication Engineering at Anna University, Chennai. He has been working as an Associate Professor in the Department of Information Technology at PSNA College of Engineering and Technology, India since June 2003. His research interests include computer networks, particularly in network optimization, multicast algorithm design, network game theory and network coding.

