Trust Based Detection of Malicious Nodes in Wireless Sensor Network

K.Sumathi[1], Dr.M.Venkatesan[2]

Abstract: The rapid growth of wireless sensor networks, it becomes a promising and one of the most interesting field in last few years. The wireless sensor networks are used in lot of applications. To ensure the security of the sensor network, the detection of malicious packet drop is very important compare to all other attacks. For this the proposed scheme describes the efficient algorithm to detect the malicious packet droppers by exponential trust. This algorithm is also depends on the maximum energy of cluster head, it leads to efficient use of clustering nodes as well as detecting a malicious nodes and creating a alert message to all other nodes in the network.

Index Terms- Wireless sensor network, malicious node, trust, cluster head.

I. Introduction

The continue changes in the Technologies, the wireless sensor network plays a vital role in our day to day life. The Wireless sensor network consists of spatially distributed autonomous sensors to monitor the environmental conditions like temperature, vibration, sound, pressure etc. Wireless sensor networks used in numerous real-time applications such as home automation, robot control, disaster relief, environment monitoring, sea labs, battlefield surveillance and automatic manufacturing. The wireless sensor network consists of low power processor, tiny memory, radio frequency module, sensing devices and limited powered batteries. The Fig1. Shows the Wireless sensor network Architecture. It consists of the following components.

Sensor Node*:* A sensor node is the most important component of WSN. The Sensor node does a multiple roles in a network, such as sensing; storing a data; routing a data to the next sensor; and processing the data.

Clusters: Clusters are the organizational horizontal unit for WSNs. The dense nature of these networks requires the need for them to be broken down into clusters to simplify tasks such a communication.

Cluster heads*:* Cluster heads are the organization leader of a cluster. The sensor node with maximum energy is chosen as Cluster heads. They often are required to organize activities in the cluster. The cluster heads are acting a watch dog in this paper. The cluster heads are updated periodically.

Terminal or End User: The data in a sensor network can be used for a wide-range of applications. Therefore, a particular application may make use of the network data over the inter-net, using a PDA, or even a desktop computer.

Base Station: The base station is at the upper level of the hierarchical WSN. It provides the communication link between the sensor network and the end-user.

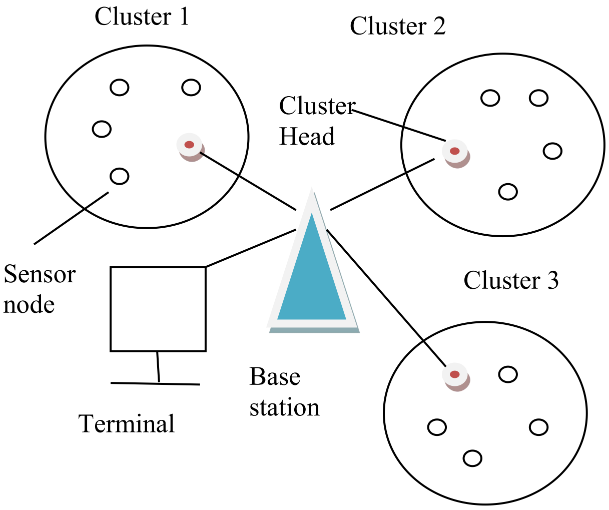

Fig 1*. Wireless Sensor Network Architecture*

The hierarchies of the Wireless sensor network's.[2] components are represented in Fig 2. In this Base station are at the level 1, Cluster Heads are at level 2 and individual cluster are at level 3

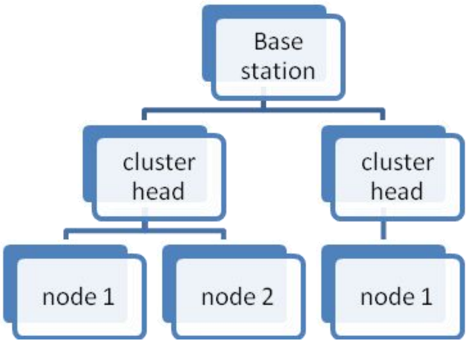

Fig 2*. Hierarchy of Wireless sensor network*

II. NEED FOR SECURITY IN WSN

The wireless sensor network are used in number of real time applications due do its wireless communications. The Wireless channel can be easily accessed by any one and any

Manuscript received Feb, 2016*.*

K.Sumathi*, AP/CSE, Anna University/ EBET Group of Institutions, Erode, Tamilnadu.*
Dr.M.Venkatesan *Principal, Anna University/ K.S.R Institute for Engineering and Technology, Thiruchengode, Tamilnadu.*

time, hence different security schemes to be integrated to transmit a data from source to sink. Such as data integrity, data confidentiality, data authentication, non-repudiation, availability, self-organization, time synchronization, access control, user privacy and continuity of service. Wireless sensor networks are characterized by denser levels of node deployment, unreliable communication of sensor nodes, compact size, limited power, computation capabilities, memory space, bandwidth and energy constraints in which sensors are being deployed in the adverse environment thus sensor nodes are vulnerable to several types of attacks . Attacks can be performed in a variety of ways. Different possible attacks created by malicious nodes are [4]

1. Bad Mouthing Attack: Propagate negative information about good nodes.
2. Good Mouthing attack: Propagate positive information about bad nodes.
3. Node Replication Attack: Create duplication of a sensor node.
4. Sinkhole Attack: Attacks nearby network traffic through compromised node .
5. Sniffing Attack: Overhear valuable data from the nearest nodes.
6. Grey hole Attack: Drop certain types of packets, which contain valuable data.
7. Hello flood Attack: Establish the attacker as the data destined for the base station through it.
8. DoS Attack: Prevent any part of WSN's from functioning correctly or in a timely manner.
9. Sybil Attack: The attacker is able to present multiple identities within the network to affect the data aggregation.
10. Selective forwarding Attack: When the attacker is in network, the decision to forward the data depends upon the attacker.

III. RELATED WORK

There are number of techniques are used to detect the malicious nodes in the network. In this section some of them are described in a few words.

In[3],Prabha R,Krishnaveni M,S.H.Manjula and K.R.Venugopal discussed to safeguard a wireless sensor network from attackers by considering trust worthiness of a node during multi hop routing. In this the author suggested that a node is trust worthy if it is communicated most of the time with other nodes in the network otherwise it is a un trusted node. The TAR algorithm is used to analyze node and through NS2 simulation the results are verified.

In[4], Yuanming Wu et. al. discussed security vulnerabilities of watchdog mechanism and trust mechanism and also examined how inside attackers could exploit them. The work was based on detection of inside attackers and their trust mechanism involved three stages: 1) node behavior monitoring, 2) trust measurement, and 3) insider attack detection.

In [5], Christhu Raj M R, Edwin Prem Kumar G, Kartheek Kusampudi, in this they described the basic methodologies for trust techniques and various research work under each category had been addressed. Sensor applications has wide range of applications and each applications been addressed an security can be addressed and implemented in each application. Providing efficient algorithm with less consumption of energy, power and memory techniques are addressed.

In [6], Marti Guili et. al. proposed a watchdog mechanism technique which worked on the concept of eavesdropping. The node can overhear all the transmissions within its radial transmission range.
The watchdog mechanism had many drawbacks due to its simple overhearing method. This mechanism was improved by A. Forootaninia and [7] where a cluster head node was fixed and buffers were used to store packets sent by the nodes.

IV. PROPOSED ALGORITHM

- Let the WSN has a collection of sensor nodes $S_{1,}$ $S_{2..}$ S_i. and assign energy E to each node
- CH- Cluster Head which is used to overhear all nodes transmission belonging to the same cluster. The Cluster Head is updated periodically.
- T_h -The Energy Timer T_h is initialized for a cluster head.
- S - Source node
- Td– The real time delay timer Tdis initialized for a node who is received the packet, its depends on the fault tolerance of the network.
- D - Destination node.
- ACK- If the packet reached the destination with in a time delay, a positive acknowledgement is transmitted from D to CH.
- NACK- If the packet does not reached the destination with in a time delay, a negative acknowledgement is transmitted from D to CH.
- Pdi- Packet dropping count

```
Begin
{
All the nodes broadcast their Energy E.
Node i with Max Energy $E_i$ is chosen as CH, &
initialize the $T_h$ for the CH.
S forwards encrypted packet to its neighbor.
The CH overhears the packet being sent to node.

Any nodes receive a packet and initialize its $T$d

 If the next node is D
 {
 D sends ACK to S
 }
 Else if the next node is not D
 {
 Initialize $Pd_i$ ;
 if node forwards the packet with in real time delay
   {
   There is no packet loss and Set $Pd_i$=0.
   }
 Else if node doesn't forwards the packet with in real time delay
   {
 There is a packet loss and Set $Pd_i = Pd_i + 1$.
 }
}
 Compute Trust value of i^th node
 $T_v$= (F ^ $Pd_i$)100
  If ($T_v$ <=$Mt_v$)
   {
 CH send Alert message to all the nodes as" i^th node is a malicious node"
   }
 If the packet does not reach D with in real time delay or no sequence
   {
   D sends NACK to the CH.
   CH sends $RT_r$ to S.
   }
   } Goto begin:
```

V. ADVANTAGES OF PROPOSED SYSTEM

1. The proposed system considered only the order in which packets are dropped by the sensor node. If total number of packets dropped by the sensor node is considered then the node initially transmitting a group of packets and built its trust value as high and gradually raises its packet dropping count. The proposed scheme avoids this problem with the help of stay above the threshold value.

2. If the sensor node not a malicious node initially and after certain period it becomes malicious then also the malicious activity of those node is detected by the proposed system.

3. The proposed system is based on both trust and as well as cluster mechanism. This leads to efficient utilization of nodes energy.

4. If the packet does not reach destination with in real time delay or no sequence then cluster head creates the negative acknowledgement and forward to the sender to retransmit the packet once again to the destination.

VI. EXPERIMENTAL RESULTS AND SIMULATION

Let us considered a WSN with 50 nodes and its Threshold trust value (MT_v) is 22.The Table1 shows how to categories a node in to either a normal or a malicious node. From the table we know that, the value of F is closer to 1 then changes in T_v is less and value of F closer to 0 then changes in T_v is more.

Table1.*Classification of node behavior based on its trust value*

Node Number	No. of Packet dropped (Pd_i)	F = 0.88	T_v=(F ^Pd_i)100	MT_v	Node status	
5	1	0.88	88	22	>	Normal node
10	3	0.88	68.14	22	>	Normal node
15	4	0.88	59.96	22	>	Normal node
20	10	0.88	27.85	22	>	Normal node
25	12	0.88	21.56	22	<=	Malicious node
30	15	0.88	14.69	22	<	Malicious node
35	23	0.88	5.28	22	<	Malicious node
40	25	0.88	4.09	22	<	Malicious node
45	30	0.88	2.16	22	<	Malicious node
50	35	0.88	1.13	22	<	Malicious node

Fig 3 illustrate the Trust Vs number of packet dropped, in which a node dropped more number of packets then its trust value is very low.

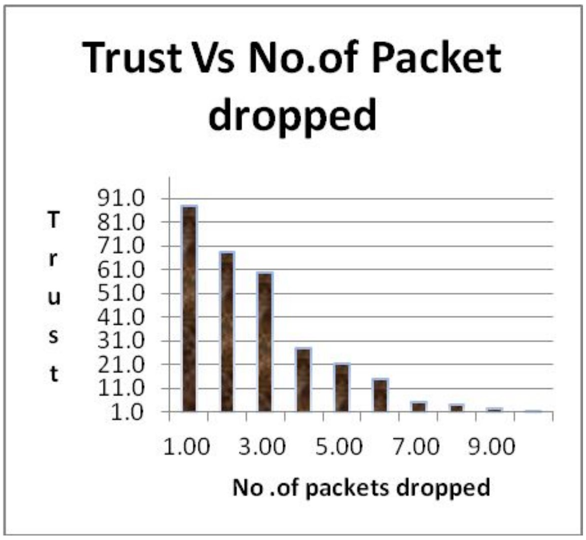

Fig3*.Trust Vs No. of packets dropped*

VII. CONCLUSION

The wireless sensor networks have much kind of applications. But they have lot of vulnerable attcks.One of the most important attack is malicious packet dropping attack. The proposed system over come this problem by calculate the trust value of the node. If the trust value of the node is decreased then the number of packet drop is also increased.

The proposed system also chose a cluster head which have maximum energy and it utilizes the cluster nodes in the network very effectively. If the packet reaches the destination within the real time delay then cluster head creates the ACK otherwise it creates the NACK.From this we know that whether the packet reached the destination within real time delay or not. The proposed system has lot of practical advantages which are discussed in the previous section.

REFERENCES

[1] Keshav Goyal1, Nidhi Gupta2, Keshawanand Singh3," A Survey on Intrusion Detection in Wireless Sensor Networks" (IJSRET) Volume 2 Issue2 pp 113-126 May 2013.

[2] S. Nishanthi**,"** Intrusion Detection in Wireless Sensor Networks Using Watchdog Based Clonal Selection Algorithm" IJREAT, Volume 1, Issue 1, March, 2013.

[3] Prabha R, Krishnaveni M,SH Manjula, KR Venugopal and L M Patnaik," QoS Aware Trust Metric based Framework for Wireless Sensor Networks.(ICCC-2015).Procedia Computer Science 48 (2015) 373 – 380.

[4] Y. Wu, Y. Cho, G. Qu, "Insider Threats against Trust Mechanism with Watchdog and Defending Approaches in Wireless Sensor Networks ",IEEE CS Security and Privacy Workshops, 2012.

[5] Christhu Raj M R, Edwin Prem Kumar G, Kartheek Kusampudi," A Survey on Detecting Selfish Nodes in Wireless Sensor Networks Using Different Trust Methodologies" (IJEAT) ISSN: 2249 – 8958, Volume-2, Issue-3, February 2013.

[6] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "*Mitigating Routing Misbehavior in Mobile Ad Hoc Networks*," Proceedings of the 6th Annual International Conference on Mobile Computing and Network-ing (MobiCom'00), pp. 255-265, August 2000.

[7] [6] A. Forootaniniaand, M. B. Ghaznavi-Ghoushchi, "*An Improved Watchdog Technique Based On Power Aware Hierarchical Design for IDS in Wireless Sensor Networks*", International Journal of Network Security & Its Applications (IJNSA), Vol.4, No.4, July 2012.

K.Sumathi received her B.E. degree in Computer Science and Engineering from Anna University Chennai in 2005 and M.E Degree in Anna University Coimbatore in 2010 and currently working as Assistant Professor in EBET Group of Institution.

Dr.M.Venkatesan completed his Ph.D in Anna University Coimbatore in 2011 and he has published 20 research papers in both conference and international journal. Nearly 10 candidates are doing their research work under his super vision and he is working as Principal in K.S.R Institute for Engineering and Technology.