MALICIOUS NODE DETECTION AND RECONSTRUCTION OF NETWORK IN SENSOR ACTOR NETWORK

KRISHNA CHOWDARY*, K.V.V. SATYANARAYANA**

* Research Scholar, Dept. of CSE, Koneru Lakshmaiah Education Foundation (KLU), Green Fields,Vaddeswaram, Guntur Dist., A.P.

**Professor, Dept. of CSE, Koneru Lakshmaiah Education Foundation (KLU),Green Fields,Vaddeswaram, Guntur Dist., A.P.

ABSTRACT

The advancement of Technology growth has developed various types of private and public applications in WSN. By the introduction of Actor node in WSN, which has an operation battery sensor, high speed computing operations is added, data processing and various components of communications. WSAN should have the capability of detecting outage of node and also have the capability to change dynamically the route with variant efficiently for providing a reliable end point – to end point communication between communication nodes in a dynamic topology change network. The proposed work should have the capability of identifying and detecting of malicious node and removal of it in WSAN. Our work is to design a framework for detection of malicious nodes in WSAN and elimination of Node in actor nodes by creating a topological structure dynamical by preparing a connectivity point of peer to peer and point to point communications. The possibility of the above is done by adding a command in actor node of WSAN for better efficiency and reliability in a network.

Key words: - *Malicious, Attacks, Packet, Actor, WSN*

1. INTRODUCTION

The advancement in Mobile network communication like Wifi, IEEE 802.11, Bluetooth or WSN, a new command based network has been emerged and is known wireless Sensor Actor network (WSAN). This Actor network has set of sensor nodes and an Actor node which monitors and provides command to the sensor nodes for effective communication from point to point network. The actor nodes have the capability of communicating with all the nodes, sensing the nodes based on load and energy and also provide computing and sensing facility of nodes.

The WSAN consists of operating sensor and storage space for command management which computes, process information and communication with components effectively. The advanced technology of actor nodes in WSN allows auto configuration, define sensor nodes preference, effective load management, can also communication in various topological structure effectively.

Attacks and security in WSN

Security is the most concern features in WSN based on function and topology structure. The usage of communication service, integration of data and network service is the main security issue in network has to be met. Security is a sensitive issues in WSAN and its application of wide range. ex. Monitoring system , tracking of object real time and targeting military issues.

Eavesdropping or passive information gathering

. In WSAN, the communication media used for various applications is unsecured on various channels. An interposerhas the capability of intercepting the communication of two valid nodes. Sensor readings that appear to be inconsistent with the remainder of the data set are the main target of the detection. Curiac*et al.* [7] proposed a detection scheme using auto-regression technique. Signal strength is used to detect malicious nodes in [8], where a message transmission is considered suspicious if the strength is incompatible with the originator's geographical position. Xiao *et al*. developed a mechanism for rating sensors in terms of correlation by exploring Markov Chain [9]. A network voting algorithm is proposed to determine faulty sensor readings.

Atakliet *al.* [10] presented a malicious node detection scheme using weighted trust evaluation for a three-layer hierarchical network architecture. Trust values are employed to identify malicious nodes behaving opposite to the sensor readings. They are updated depending on the distribution of neighboring nodes. An improved intrusion detection scheme based on weighted trust evaluation was proposed in [12]. The mistaken ratio of each individual sensor node is used in updating the trust values. Trust management schemes have been proposed in routing and communications [13]. Some efforts are also being made to combine communication and data trusts [14]. However, malicious node detection in the presence of various types of misleading sensor readings due to the compromised nodes have not been deeply investigated. In addition, the resulting event detection performance has not sufficiently been taken into account in malicious node detection.

In this paper, we present a neighbor-based malicious node detection scheme for wireless sensor networks. Malicious nodes are modeled as faulty nodes that may intentionally report false data with some intelligence not to be easily detected. The scheme identifies malicious nodes unless they behave similar to normal nodes. Confidence levels and weighted majority voting are employed to detect and isolate malicious nodes without sacrificing normal nodes and degrading event detection accuracy

Attack of Flood : It is process of creating a new connection even the resource are exhausted it keeps on searching .
Malfunctioning Node – it is caused due to dropping of packets at high rate in a network ,which delays the network traffic on topology structure. If these nodes are not rectified they will change the overall performance of network.

Injection Message
This type of attack occurs , when dummy message are introduced in the network with false information

Outage node - this type of attack occurs when packages are communicated between nodes, this attack alters the structure of the network and transmit the packet in a wrong direction
Corruption of Message – This type of attack occur in between two nodes, a new intruder will join in between the two legitimate node, it changes the packet data and transmit to the another node. The result of it leads to corrupted data.

Node fault or false – It is a dangerous attack occurs in a network and also damage the network communication by blocking the route and misguiding the exchange of data in a network.

Replication of node – A new malicious node will be added in the network which copies the existing node identity of the sensor node. This node will inject the unwanted data and misroute the traffic of network and security in WSN.

Jamming Attack
Using radio frequency signals , sensor node network can be disrupt and certain nodes in the network can be block listed.

2. 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.
We come across various methods used for identification of malicious node in WSN. Our work has been done based on the study of existing works developed and proposed by few authors.
K.R. Venugopal[3] Suggested how to safeguard the WSN nodes from the introducers when they attack the node for data, also suggest how to identify the Malwares nodes in multi hop network. He developed an algorithm TAR which is used to analyze the nodes in WSN using NS2 . His works provide better results when compared to the existing methods in identification of fault nodes in WSN.
Wu Yaunming[4]proposed a watchdog technique in identification for checking of nodes which are effected by the attackers and also exploited the function and behavior of exploiters.he also proposed how a mechanism of trust for monitoring in 3 stages a) measurement of trust b) detection of inside attacks c) behavior of node

Prem Kumar[5]he has proposed and suggests to develop a trust technique for various type of applications in sensor network based of the category of network and its applications, also suggested the addressing capability on security and trust management. He proposed an algorithm related to trust and efficient which produce less consumption of energy, memory management technique on each nodes and power management.

Guilie[6], developed an algorithm based on watchdog, it is used to identify the sets of sensor node in a wide range and identifies the fault nodes and the attacks that are occur in the WSN. This method proposed has various drawbacks. But this method can be used on for some range for better accuracy of identification of malicious nodes.

Foorootaninias[7], proposed an algorithm which provides the extension of the previous method of using watchdog timer circuit in identification of fault nodes, this much he propose gives better results compare the above.

3. PROPOSED WORK

Proposed an Actor Sensor network node consist of modules

Request reply module
Identification and detection module
Communication module
Dynamic path creation module
Packet monitoring module

Request reply module: - In WSAN network, actor nodes possess set of command, this commands are used to monitor and identify the fault nodes in a network. The actor nodes have a memory unit which possesses command among the command of its possibility, a command Request and reply command.
Command Request () – The actor node broadcast the packets on to the network of its neighbor whereas the sensor node transfers the request to its neighbor and so on. This process of broadcast communicates to all the sensor nodes from source node to the destination node. Then the command reply () re-reply the sensor node in the reverse way to the source. It uses the process of broadcast and reply method in creating a path from source to destination. This process is controlled and managed by the Actor node in a network with sink nodes in multi-path wireless sensor network.

Detection and Identification module – When the Actor nodes in WSAN do have received any acknowledgement from the sensor nodes, It identifies or notifies that any error or a problem has occurred in a sensor node. To verify the problem of occur, the actor node broadcast a command detect (), which identifies the fault node from the base of request-reply command().

The sensor node command performs the following on the fault nodes

Check for the Energy failure of sensor node
Check for the traffic delay of the node
Check for the topology structure
Load check on the sensor node.

The sensor actor nodes transmit the command on the sensor node this command verifies the following aspects on the sensor nodes

If the failure of energy- it can be regained by the actor node in transmitting energy to the sensor nodes.

If the failure is on traffic delay on the sensor node, then the actor node issues a command to distribute the traffic balance among the sensor nodes.

If the failure is on topology structure – The actor nodes will reconstruct the topology structure dynamical by eliminating the effected node.

Dynamic path creation: The actor node provides a function in WSAN has the capability of creating a topology structure dynamically based on the behavior of the network and no of fault node occurred in a network from point-point communication.

Packet monitoring module : To monitor the packets in a network Actor node issues set of command to check the packet status, packet collision occurred in a network , packet no reply case occurs at the fault nodes, life of the packet , rate of transmission of packet and strength of the topology structure.

PROPOSED ALGORITHM

start
{
Every node is broadcasted for energy check

If energy is less than the actual, actor node distribution the energy to the sensor nodes.
Let assign the value to I as ch

Actor node then forwards S packet to the neighbor of the sensor nodes

*Ch is overhears to by the neighbor when forwards *
All nodes are received with packets from the initialize node source of d
All the nodes broadcast their Energy E.

```
Node i with Max Energy Ei is chosen as CH, & initialize the $i^{th}$ 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 ᵊd.
Check for identification of node D if it is next
{
    Ack is sent to S from D
}
If the next node is D
{
    D sends ACK to S
}
Else if the next node is not D
{
    If not D the next node {
        Assign pdi
        Actor node in WSAN broadcast a delay function
        {
            If it identifies no loss of packet it initializes pdi to 0
        }
        Else if a check for broadcast the packet in time delay
        {
            A loss of packet is identified and assigns value of pdi +1
        }
    }
Computation of value is check for trust nodes of i
$Tv= (F^{pdi}) * 100$
If ($Tv <= Mty$)
{
    Then the actor nodes broad the commands, which send to the neighboring nodes as effected and those nodes are attached with Malicious node
}
If malicious nodes are identified restructure of topology structure has to be done
WSAN forwards a command for re-built of dynamical topology with the neighbor node, and eliminate i th effected node
After building the topology structure, then energy function is checked, load of each node is checked, traffic is verified by the Actor node in WSAN
}
A check for received of nodes to the distention D in real time based on sequence or delay factor
Recall start.
```

Table 1. Show the node behavior of Trust

Number of nodes	Dropped packet count Pdi	F=0.89	Tv=(F^Pdi)	MT	Status of node
4	**1**	**0.89**	**89**	**23**	**>Normal**
8	**3**	**0.89**	**68.16**	**23**	**>Normal**
12	**4**	**0.89**	**59.64**	**23**	**>Normal**
16	**10**	**0.89**	**27.88**	**23**	**>Normal**
20	**12**	**0.89**	**21.58**	**23**	**<=Malicous node**
24	**15**	**0.87**	**14.69**	**23**	**<Malicious node**
28	**23**	**0.89**	**4.08**	**23**	**< Malicious node**
32	**25**	**0.89**	**2.18**	**23**	**< Malicious node**
36	**30**	**0.89**	**4.09**	**23**	**<Malicious node**

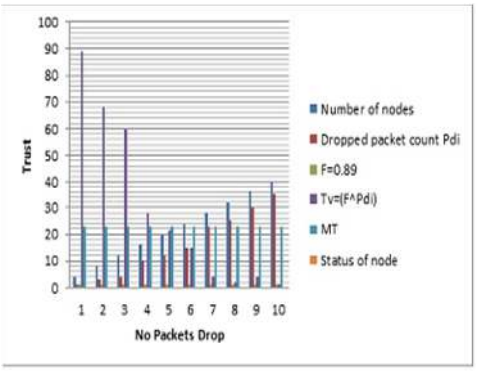


FIGURE 1. Show the detect of Malicious node in WSAN

The proposed is used to

1. Identify and detect correctly malicious nodes in WSAN, The management of Trust is maintained by the Actor node in a sensor network.
2. Prepare a Routing path dynamically among the other un-effected nodes

3. Check for the traffic efficient of the node
4. Re-structure the topology structure based on load and energy efficiency management.

4. EXPERIMENTAL RESULTS

We have considered 50 nodes, threshold value MTv is 23. Table 1 mentioned above shows the node categorization with normal case or malicious node. According to the observation , if the value of F is nearly to 1 , there is a change in Tv which is lesser and F value closer to 0 , then Tv is assumed to be more.

5. MALICIOUS NODE DETECTION

In our neighbor-based detection scheme, each sensor node detects malicious nodes, along with faulty nodes, locally using only the sensor readings of its neighboring nodes. A weighted majority voting using the confidence levels as weights is used to detect malicious nodes. The pro-posed detection scheme can be depicted as follows.

Malicious Node Detection

1) Given sensor reading x_i^k , obtain y_i^k and deter-mine b_i^k , and perform variation test for suck-at-0 fault detection

2) Receive b_i^k and F_j from neighbors (periodic). Send

an alarm to neighboring nodes (event-driven)

3) Compute and make a decision D_i

$$M_0 \square \square_{j \square 1}^{d_i \square 1} w_{ij} \square 1 \square b_j^k \square \text{ and }$$
$$M_1 \square \square_{j \square 1}^{d_i \square 1} w_{ij} b_j^k$$

$D_i = 1$ (*i.e.* an event) if $M_1 > M_0$

4) Update the confidence levels w_{ij} accordingly

In Step 1, most wrong data due to transient faults are locally corrected and hence false alarms can be greatly reduced without incurring any internode communications. In addition, the variation test is conducted for the sensor readings during the cycle T_c. In Step 2, neighbor communications are used to perform periodic checking (in the periodic mode). In the event-driven mode, however, only the nodes with b_i = 1 report an alarm to neighboring nodes to initiate an event-driven detection. Step 3 per-forms a weighted majority voting to make a decision on an event, where M_1(M_0) is the sum of weights of nodes with b_{ij} = 1(0) and d$_i$ is the node degree of v_i. The confidence levels are reflected in the decision making process. In Step 4, all the weights, w_{ij} , are updated. Updating the weights in such a way that malicious nodes can be effectively removed from the network is important.

Our updating policy differs depending on the decision made on an event. In the case of no-event, the weight w_{ij} is updated as shown in **Table 2** , where F_j denotes the fault status of v_j. The confidence level of node v_j, w_{ij}, is increased by β only when v_j is fault-free (*i.e.* $F_j = 0$) and it belongs to the majority group. It is decreased by αoth-erwise. Here α and β have to be properly chosen to optimize the performance.

In the case of an event, the weight w_{ij} is updated as shown in **Table 3**. The only difference is the third row where the confidence level remains unchanged since the exact boundary of an event region is unknown.

Table 2. Updating w_{ij} at node v_i in case of no-event.

D_i=b_j	F_j	w_{ij}
yes	**0(good)**	**min($w_{ij} + \beta$, 1)**
yes	**1(faulty)**	**max($w_{ij} - \alpha$, 0)**
no	**0(good)**	**max($w_{ij} - \alpha$, 0)**
no	**1(faulty)**	**max($w_{ij} - \alpha$, 0)**

Table 3. Updating w_{ij} at node v_i with D_i = 1 in case **of an event.**

D_i=b_i	F_j	w_{ij}
yes	**0(good)**	**min($w_{ij} + \beta$, 1)**

yes	**1(faulty)**	**max(w_{ij}–α, 0)**
no	**0(good)**	**no change**
no	**1(faulty)**	**max(w_{ij}–α, 0)**

Each sensor node v_i also updates its own confidence level w_{ii} in the case of no-event as follows.

$$w_{ii} = \begin{cases} \max(0, w_{ii} - \alpha) \text{ for } b_i = 1 \text{ or } S_i = 1 \\ \min(1, w_{ii} + \beta) \; for \; b_i = S_i = 1 \end{cases}$$

In the above expression, $S_i = 1$ means that the readings at node v_i do not satisfy the minimum variation require-ments, indicating a potential stuck-at-0 fault. Fault status of node v_i, F_i, initially 0 (fault-free), is set to 1(faulty) when w_{ii} reaches 0. Once it is set to 1, it will stay there if no recovery action is taken.

Malicious nodes behaving like a normal node can hardly be detected. However, it does not cause a signifi-cant problem. Malicious nodes with some intelligence might behave differently from normal and faulty nodes to remain undetected. The proposed scheme is focused on accurately detecting such malicious nodes and isolating them from the network. Consequently, it achieves high performance for a wider range of p_{ma}.

6. SIMULATION RESULTS

Computer simulation is conducted to evaluate the effectiveness of our malicious node detection scheme and the resulting event detection accuracy. In the simulation, we randomly deployed 1024 sensor nodes in a square area. The transmission range r is chosen to set the average node degree d to be 12. In addition, an event region is assumed to be a circle with radius r (*i.e.* the same as the transmission range).

Transient faults, permanent faults, and malicious nodes are generated randomly and independently. In the case of permanent faults, they are generated uniformly during the first 10 cycles of operation. In the case of no event, malicious nodes are assumed to report against the actual readings with probability p_{ma}. On the other hand, they are assumed to report a 0 when they are in an event region, to estimate the event detection performance in the worst case.

Two metrics, malicious node detection rate (MDR) and misdetection rate (MR), are defined to evaluate the pro-posed malicious node detection scheme. MDR is defined to be the ratio between the number of detected malicious nodes and the total number of malicious nodes. MR is defined as the ratio of normal nodes determined to be faulty to the total number of normal nodes. The reason for not defining MR with respect to malicious nodes is that malicious nodes behaving like a normal node (*i.e.* reporting correctly most of the time) do not harm at all until they change their behavior.

Two additional metrics, event detection accuracy (EDA) and false alarm rate (FAR), are used to evaluate the resulting event detection performance. EDA is de-fined as the ratio between the number of events correctly identified and the total number of events generated. FAR is the ratio of the number of nodes reporting a 1 to the total number of nodes, in case of no-event

We first performed simulation to estimate MDR and MR for four different values of p_m, 0.05, 0.10, 0.15, and 0.20, when $p_p = 0.1$, $p_t = 0.1$, $p_{ma} = 0.4$. The results, after 50 cycles of operation, are shown in **Table 3(a)**, where α 0.2 and $\beta = 0.05$ are chosen. For comparison purposes, we also performed simulation for $\alpha = \beta = 0.1$ (**Table3(b)**). MDR in **Table 4(a)** is high while MR is negligiblysmall. On the other hand, MDR in **Table 4(b)** is extremely low due to the fact that confidence levels lost are quickly recovered. As can be seen in **Table 4**, the value

of $\frac{□}{□}$ has to be assigned properly to achieve high MDR,

while maintaining low MR. If $\frac{□}{□} = 4$, for example, a

malicious node sending an alarm every five cycles in case of no-event recovers its confidence levels, and is thus unlikely to be detected. Such a high MDR in **Table3(a)** is obtained since$p_{ma}$is set to 0.4 in the simulation.

The confidence level of a malicious node becomes lowered with time to reach the lower bound if report a 1 every four cycles on average in the case of no-event. Even in that case, $\frac{\square}{\square}$ = 4 is sufficient to lowerthe confidence levels of malicious nodes to be eventually detected.

In **Figure 3**, the resulting EDA is shown for various values of p_m for the same values of α and β. FAR for the two maintains more persistent and stable performance compared to the other pair (0.1,0.1) as p_m increases.differentcases are almost the same and very close to 0, and are not shown in the figure. The first pair (0.2, 0.05)

In order to see the importance of the values of α and β in malicious node detection, we conducted the same

Table 4. MDR and MR for various values of p_m when $p_p = p_t = 0.1$. (a) $\alpha = 0.2$, $\beta = 0.05$; (b) $\alpha = 0.1$, $\beta = 0.1$.

(a)

	p_m= 0.05	0.10	0.15	0.20
MDR	0.961	0.963	0.961	0.958
MR	0.009	0.007	0.007	0.008

In order to see the importance of the values of α and β in malicious node detection, we conducted the same

Table 4. MDR and MR for various values of p_m when $p_p = p_t = 0.1$. (a) $\alpha = 0.2$, $\beta = 0.05$; (b) $\alpha = 0.1$, $\beta = 0.1$.

(b)

	p_m= 0.05	0.10	0.15	0.20
MDR	0.961	0.963	0.961	0.958
MR	0.009	0.007	0.007	0.008

(b)

	p_m= 0.05	0.10	0.15	0.20
MDR	0.036	0.013	0.023	0.013
MR	0.000	0.000	0.000	0.001

simulation for five different values of p_{ma}. Two pairs of (α, β), (0.2,0.02) and (0.2,0.05) are chosen for compari-son purposes. For p_p = 0.1, p_t = 0.1, and p_m = 0.2, the resulting MDR and EDA are shown in **Figure 4**. MR and FAR are not included since they are close to 0 for the cases under consideration.

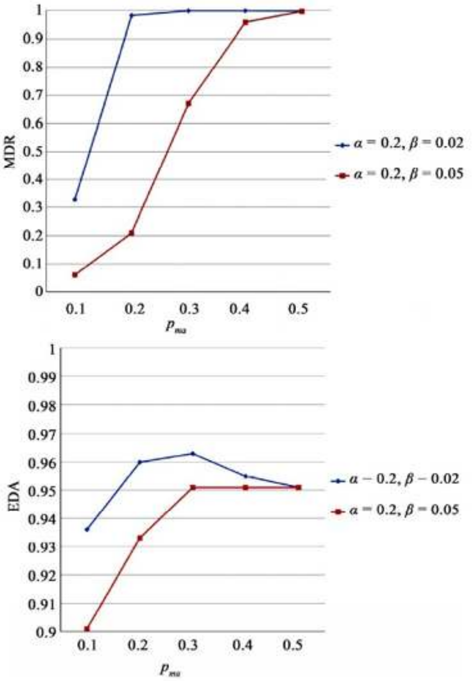
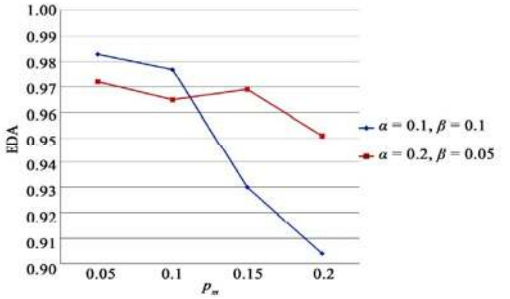


Figure 3. EDA for two different pairs of α and β

Figure 4. EDA for two different pairs of α and β

As can be seen from **Figure 4** , MDR for (0.2,0.02) is significantly higher than that for (0.2,0.05) for relatively small values of p_{ma}. These improvements have been madep_t= 0.1, if $p_{\ ma}$is close to 0.1, malicious nodes behavelike a normal node, and thus they can hardly be detected without increasing the detection time or sacrificing some normal nodes. Filtering transient faults lowers p_t in such a way that a considerable amount of malicious nodes can still be detected.



We then conducted simulation to see the performance gain we can obtain by removing stuck-at-0 nodes. The proposed scheme has provisions to detect such faults as long as the resulting sensor readings are confined to a

p_p	EDA		FAR	
	Proposed	MV	Proposed	MV
0.2	0.957	0.930	0.002	0.021
0.4	0.928	0.913	0.014	0.114

relatively small range of normal values over time com-pared to normal sensor nodes. Since not all stuck-at-0 faults meet the requirements, the scheme is partially effective. The simulation results for various values of p_p when stuck-at-0 faults are isolated are shown in **Table4(b)**, whereα= 0.2,β= 0.05 andp_{ma}= 0.4 are chosen.For comparison purposes the results when stuck-at-0 faults remain in the network are shown in **Table 4(a)**.

As far as MDR and MR are concerned, there are neg-ligible differences in performance. A notable difference in EDA, however, is observed as p_p increases. Removing stuck-at-0 faults is desirable when EDA is concerned.

Finally, we evaluated the proposed scheme in terms of EDA and FAR by comparing its performance with those of majority voting (MV). Since MV is not for malicious node detection, MDR and MR are not included in the comparisons. The results for two different values of p_p when $p_m = p_t = 0.1$ are shown in **Table 5**, where $\alpha = 0.2$,

$\beta = 0.05$, and $p_{ma} = 0.4$ are chosen for our scheme. The proposed scheme outperforms the majority voting with respect to EDA and FAR.

Table 4. MDR, MR, EDA, and FAR for various values of p_p when $p_m = p_t = 0.1$. (a) Without removing stuck-at-0 faults; (b) After removing stuck-at-0 faults.

(a)

	p_p= 0.1	0.2	0.3	0.4
MDR	0.962	0.952	0.953	0.954
MR	0.007	0.009	0.013	0.021
EDA	0.969	0.915	0.819	0.664
FAR	0.000	0.001	0.002	0.004

Table 5. EDA and FAR for two different values of p_p when p_m=p_t= 0.1.

(b)

	p_p= 0.1	0.2	0.3	0.4
MDR	0.963	0.955	0.953	0.941
MR	0.007	0.009	0.014	0.025
EDA	0.965	0.957	0.935	0.928
FAR	0.001	0.002	0.004	0.014

The above simulated in NS2 shows the detection of attacks occur in WSAN, The actor node sends a command, using the command driven mode it identifies the attacks on the node

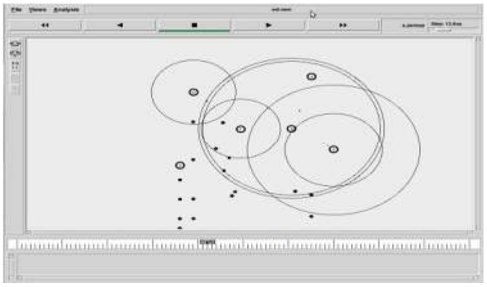


Figure 5: Remove of Attack from WSAN

Figure 5, above show the remove of attacks occur by releasing a command for eliminating the attacked nodes by the Actor node in WSAN.

6. EVALUATION OF PERFORMANCE

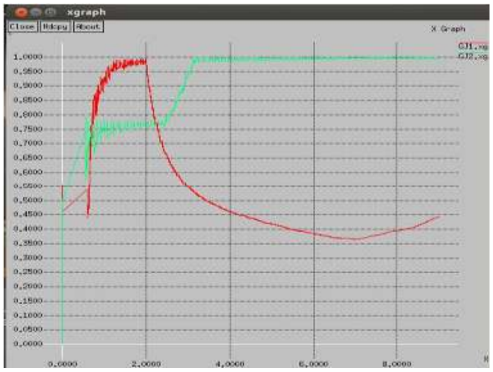


Figure 6. Time Vs Delay

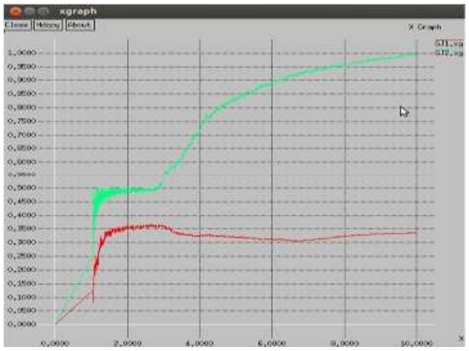


Figure 7 of Packet Delivery Factor Vs Time

either SI (MKS) or CGS as primary units. (SI units are encouraged.) English units may be used as secondary

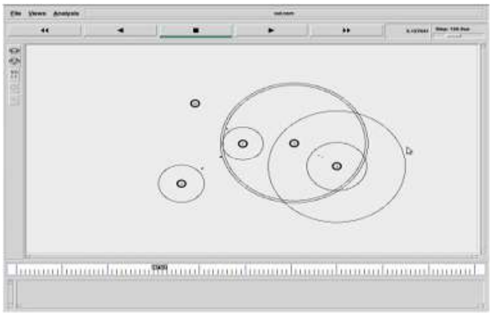


Figure 8 No of Malicious node Attacks

Figure 8 above show the various types of attached occur in WSAN, using the command mode function stored in the actor nodes these malicious node attacks can be blocks.

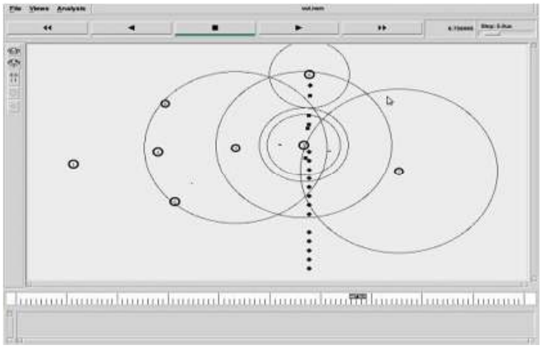


Figure 9 Attacked Node Removal

Figure 9 , above show the remove of malicious nodes from the attacks. The Actor node restructures the configuration of the topology by eliminating the effected nodes.

Measure of Performance Evaluation

The figure below shows the indication of malicious nodes based on the nodes structure with line red. Line green indicates the absence of malicious node.

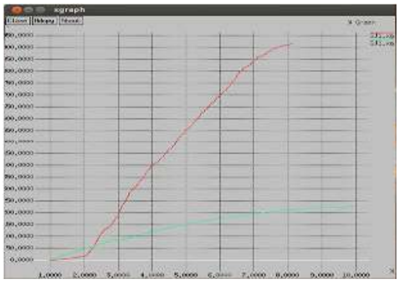


Figure 10. Time Vs Delay

The factor that effect the structure of WSAN is mention with

Delay : It is the average mean value taken by the packets to reach the destination is called as time delay.

Packet Fraction Delivery: It is the mean ratio of packets reached to the destination to that of packets sent from the source.

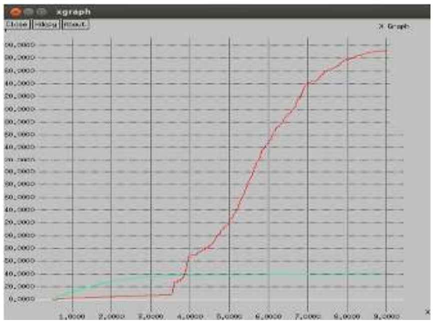


Figure 11 Time Vs Packet Delay Factor

7. CONCLUSION

Our work mainly focused on identification of fault node which is affected. After detecting the node which is affected, the Actor node in the WSAN provides command, this command will regain the effective structure of topology network in preparing a end-point to end-point communication. our work proposed a neighbor-based malicious node detection scheme for wireless sensor networks. Malicious nodes are detected in the presence of faults and events without sacrificing normal nodes. They are modeled as faulty nodes that can arbitrarily modify sensor readings and behave intelligently not to be easily detected. Confidence levels are used to estimate trustworthiness of sensor nodes during normal operation. They are reflected in the decision making process at each sensor node. Two parameters for updating the confidence levels are employed to distinguish malicious nodes from normal modes as long as they behave differently from normal nodes..

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,SHManjula, 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, KartheekKusampudi," 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] Haowen Chan and Adrian Perrig, "Security and Privacy in Sensor Networks", IEEE, October 2003, pp. 103-105.

[8] Curiac, D.-I., Plastoi, M., Banias, O., Volosencu, C., Tudoroiu, R., Doboli, A.: "Combined malicious node discovery and self-destruction technique for wireless sensor networks". Int. Conf. on Sensor Technologies and Applications, 2009, pp. 436–441

[9] Lazos, L., Hirloc, P.R.: "High-resolution robust localization for wireless sensor networks", IEEE J. Sel. Areas Commun., 2006, 24, (2), pp. 233–246

[10] Anjum, F., Pandey, S., Agrawal, P.: "Secure localization in sensor networks using transmission range variation". IEEE Int. Mobile Ad Hoc and Sensor Systems Conf., November 2005, vol. 9

[11] Anthony D. Wood, John A. Stankovic, "Denial of Sevice in Sensor Network", IEEE 2002.

[12] S.H.Jokhio, I.A.Jokhio, A.H.Kemp, "Node capture attack detection and defence in wireless sensor networks", IET 2011.

[13] http://www.dees.unict.it/users/bando/files/wsn.pdf ; September ,2015, 14:02 PM

[14] http://www.ijareeie.com, August 2014: 15:09:10

[15]http://ict4dconsortium.rhul.ac.uk/elgg/action/file/download?file_guid=7764http://nile.wpi.edu/NS/, December ,2013 ; 17:05 pm

[16] Z.A.Baig, "Pattern recognition for detecting distributed node exhaustion attacks in wireless sensor networks", Elsevier 2010, pp. 468-484.

[17] ZHANG Yi-ying, LI Xiang-zhen, LIU Yuan-an, "The detection and defence of DoS attack for wireless sensor network", Elsevier 2012, pp. 52-56.