Catching Packet Droppers using Behavioral based Anomaly Detection in Wireless Sensor Network

Shikha Namdeo [1]
M.Tech Scholar, Department of Computer Science & Engineering
LNCT,Bhopal, India

Dr. Sadhna K. Mishra[2]
Professor, Department of Computer Science & Engineering
LNCT,Bhopal, India

Dr. Vineet Richhariya[3]
Professor & Head, Department of Computer Science & Engineering
LNCT,Bhopal, India

***Abstract*—Security threat and routing holes in wireless scenario are more frequent than other networks. Lack of infrastructure and centralized monitoring using limited battery power are the crucial point. Attackers can easily launch an attack to consumed resources of wireless network such as battery power packet dropping attack in sensor network. In such exploiting condition an antagonist node may launch various attacks to disturb the communication in WSN. Amidst of such attacks packet dropping and modifier are the most prevailing attacks. In packet dropping attack compromising nods starts dropping each and every packet pass from him (node) or modify the packet before forwarding in a later attack. In wireless sensor network, there are so many challenges and issues as already been discussed and proposed. The main challenges are how to provide maximum lifetime to network and how to provide robustness to network. In sensor network, the energy is mainly consumed for three purposes: data transmission, signal processing, and hardware operation. In this article we have Propose a machine learning based mechanism to identify the routing holes on wireless sensor network. The concept lies on social behavior of the human society in which individual's behavior is the benchmark to decide his authenticity in the network. Proposed system works on the concept of the anomaly detection due to unlabeled information produce by the sensor nodes. The overall objective of this research article is to identify packet dropper and modifier in wireless sensor network against the set of qualitative performance metrics.**

***Keywords*— Control Overhead, delivery ratio, energy remains, Machine learning, sensor, wireless sensor network, WSN, packet dropper.**

I. INTRODUCTION

Sensor network or Wireless sensors are extensively applied climate observance in remote areas for cave studies of the atmosphere, sea waves study like tsunami alert as well as widely applied on wildlife tracking and so forth. Sensor nodes are one of the primary elements that sense the locale and monitor it, observe the consequences, collecting them to process the information and directed en route to a sink node. In WSN another important entity is sink node that will be a router (gateway), an AP (access Point) or Base station (BS), or a node having storage, or just a querying node [1]. Being easy to use and deploy and having inexpensive installation charge, autonomy quality sensors networks are widely deployed on unreachable and in hostile habitat to monitor and gather the information related to that environment.

Security needs of WSN in such network due to lack of physical protection on it. The Attacker can easily launch an attack in such scenario and disrupt the communication. In such exploiting condition an antagonist node may launch various attacks [1] to disturb the communication in WSN. Amidst of such attacks packet dropping and modifier are the most prevailing attacks. In packet dropping attack compromising nods starts dropping each and every packet pass from him (node) or modify the packet before forwarding in a later attack.

It defines the intrusion as any set of actions that are attempting to compromise the main components of the security system [6]. Weak infra structure of wireless communication helps adversaries to perform variety of passive, active and stealth type of attacks easily. In passive mode, an adversary or attacker silently observe the radio channels in order to capture data, gain security credentials, or to collect confidential information to derive the credentials. In active attacks, adversaries may eavesdrop on the network transmissions, capture and read the contents of data packets send by sensor nodes. A protection scheme detects the different type of attacks and sends the report to base station or all nodes in network. It uses all nodes or some special nodes to detect these types of attacks. These nodes co-operate each other to take the decision and finally send the report to the base station. It requires lots of communication between the nodes. If adversary can trap the message exchanging between the nodes then they can easily tamper the messages and send the false information to the other nodes.

In wireless sensor network, there are so many challenges and issues as already been discussed and proposed. The main challenges are how to provide maximum lifetime to network and how to provide robustness to network. In sensor network, the energy is mainly consumed for three purposes: data transmission, signal processing, and hardware operation. It is said in [5] that 70% of energy consumption is due to data transmission.

In packet dropping attack compromising nods starts dropping each and every packet pass from him (node) or modify the packet before forwarding.

Propose a machine learning based mechanism to identify the routing holes on wireless sensor network. The concept lies on social behavior of the human society in which individual's behavior is the benchmark to decide his authenticity in the network. Proposed system works on the concept of the

anomaly detection due to unlabeled information produce by the sensor nodes.

The overall objective of this research article is to identify packet dropper and modifier in wireless sensor network against the set of qualitative performance metrics.

The specific goals of this research work:

- Identify the intrusion on the basis of the node energy remain as a metric.
- To extends the limitation of conventional wireless Intrusion Detection System (IDS) with the help of integrating behavior metrics of node of to determine Selfishness and black hole nature.
- For effective and accurate results of propose security system behavioral data must classify properly. Soft computing and learning methods produces the most accurate results. Propose system has adopted the SVM (Support Vector Machine) for behavioral classification to identify the packet droppers in sensor network.
- Use of learning computation (SVM) the false ratio has been extensively reduces in propose system.

Rest of the paper organized as follow, section 2 describes related terminology and background work, and section 3 focuses on related work in WiMax area. Section 4 discusses the proposed solution; finally section 5 gives the conclusion of this paper.

II. Related Work And Problem Identification

Before presenting the proposed methodology first we want to address the problem in existing system –

Problem has been identified in [1]:

a. Author has proposed a good approach but it restrict to DAG topology.
b. Author has used the concept of key exchange which seems computation overhead in such a battery constraint environment.

Problem has been identified in [2]:

a. Whereas author [2] has address the BATTERY power disasters in wireless sensor networks.
b. Author of [2] has concentrate his research are on self Healing i.e. energy utilization in case of failure. Author has proposed a Mobile agent based scheme inspired from biological science (autonomy and self healing nature of cells to develop agent as a replica) to make WSN nodes as a self healing entity while there is battery drainage.

Author has used the concept of mobile agent which is good but restricted to the specific areas like remote station where monitoring is complex and infeasible like changing the battery power.

Mobile agents are a good concept because they are autonomous (self executable) and social in nature but their management and security is the bigger challenge.

Problem has been identified in [3]:

Instead of proposing a new mechanism there is also a evaluation is required to analyze the impact of the existing method with some common metrics, author [3] has do the same in the article in which existing IDS techniques (whether they are anomaly based or signature one) has been chosen to test their effectiveness in WSN. Author has proposed some guidelines to strengthen the IDS technique with analyzing their impact in WSN.

Problem has been identified in [4]:

Author of [4] has used the anomaly detection technique of IDS to detect suspicious activity by integrating a classifier in the node i.e. SVM (support Vector Machine) on it.

Author has used the concept of SVM for detecting attacks in WSN. We have chosen author concept for enhancement in the research areas.

Proposed system will design to detect and prevent packet dropper nodes in the WSN. Proposed scheme is the enhancement of the author's [1] and [4] method.

In this paper some more metrics will be needed to enhance SVM based classifier mechanism which we will discuss in our proposed mechanism.

Author has applied the proposed behavior based mechanism on sink node, but our method has been applied to each node which reduces the computational overhead.

Proposed system will consider two types of attack which is more related to packet dropper attack-

i. Selfish Node
ii. Black Hole

III. Proposed Algorithm

In wireless sensor network scenario the greatest problem that has been seen now a days is a security threat such as packet dropper attack resulting the battery consumption and finally disrupting the sensor networks working.

Proposed method's core concept is anomaly detection technique of IDS in which the deviated profile will be treated as anomaly. For the base profile the normal transmission profile of the node will be chosen during packet transmission.

The general idea of the proposed works as follow-

To enhance the performance of the above mentioned scheme we have integrated the idea of classification of the behavior of Selfishness and black hole nature using support vector machine.

Nodes are planned to expand the maximum reimbursement from the networks even as safeguard their own resources like hardware, battery power or bandwidth. Selfish nodes do only outgoing from their own. Hence they only send data packets to other node as a source. While after receiving packets from other nodes they refused to cooperate. Consequently, they start dropping of packets or refuse.

Proposed solution is based on anomaly detection concept of IDS by applying behavioral normality and abnormality in

nodes of the MANET during transmission (data or route discovery packets) –

i. Build normal profile of Nodes during communication based on their behavior with help of Metrics like Packet Delivery Ratio and packet Drop ratio, Routing overhead, End-to End Delay, Total no of Hello message, Energy_Remain of the node.

ii. Then build anomaly detector by applying Behavioral Classifier to classify the nodes into normal and flooded. For achieving these following rules has been used:

iii. Determination of Metrics use in Proposed Solution

- Pkt_Del_R (Packet Delivery Ratio)

  Pkt_Del_R = No. of packets transmitted/Total no. of packets receive

- RO (Routing Overhead)

  RO = Number of Routing Packets Sent / Number of Received Data Packets

- Total no of Hello_msg transmitted
- Enrgy_Remain

Has work as a benchmark for identification of selfish node in WSN. The following proposed methodology we have develop to restrict the selfishness of a node in wireless infrastructure less environment –

i. Capturing/recording the behavior of each node (using packet delivery, modification and route modification ratio of a node).

ii. Applying the threshold mechanism on each node to restrict the flooding of unnecessary route control packets in the network (Using monitoring pr supervision of behavior) with help of support vector machine (SVM).

Same mechanism will also apply to detect black hole attack and causing node for the same. The main concern property in black hole will be the response of packet delivery ratio (Packet_Del_R) of the node.

Proposed solution is based on anomaly detection concept of Intrusion Detection System. In this proposed method the behavioral (during transmission) metrics of the Sensor nodes works as a anomaly benchmark. Hence behavioral data has been used to check normality and abnormality of the nodes in WSN (Wireless Sensor Network) during transmission (data or route discovery procedures). Our proposed anomaly detector paradigm work as follow to defend against packet Dropper's or Selfish attack and provides the better solution which is efficient, scalable, energy saving and robust–

1. Building behavioral profile of Nodes while communicating in sensor environment. As it knows that anomaly detection approach requires one benchmark profile i.e. normal profile to compares while detecting the attacks. For this first proposed system has build normal profile of sensor nodes using simulation. For this behavioral of the nodes has been collected from the simulation environment of normal condition. Afterward the profile mtrices has been evaluated/derives like packet delivery ratio, routing overhead, No_Hello_msg (from MAC layer) and energy remains. These all are applied to build normal profiles. To achieve this, generated XML files (trace file of NS-3 simulation) has been used to derive metrics.

Algorithm –I

a. Built the WSN topology on NS-3.18.

b. Start the Simulation and build the record the transmission data i.e. of behavioral profile of the sensor nodes.

c. Collect the behavioral statistics into .xml or .tr (trace) file format and also record the routing overhead and number of Hello messages of each node

d. Parse .xml file to determine the metrics related to sensing nodes

e. Determine the value of Pkt_Del_R, RO , No_Hello_msg and ER and for each node

(Note: the value of ER and No_Hello_msg has been extracted using test files generated during simulation)

2. Then training of anomaly detector has been applying with the help of SVM classifier on behavioral of nodes to classify the nodes to check t whether there has been packet dropper/selfish attack or not. For better understanding the normal and attack has been labeled as "d" for 'dropper' and "a" for 'authenticate' node in support Vector Machine (SVM).

Table 1: Algorithm to classify the sensor nodes

Algorithm II: Behavioral Classification to Detect Packet Dropper

```
grp={}; // Array variable to store two group authenticate or packet dropper

    for i=1:node
      if(pkt_del_r(i)>=0.7)
        grp{i}='A' //authenticated Node
      elseif((pkt_del_r (i)>=0.5 & pmir(i)>=0.3))
       grp{i}='M' //paket Dropper
      elseif(((pdr(i)<0.5 &pmir(i)>=0.5)||pmir(i)>=0.7)
        grp{i}='M'
      else
        grp{i}='A';
      end
      if((pdr(i)<0.5) & (er<0.03) & (pmir(i)>=0.3))
        grp{i}='M'
      elseif((pmir(i)>=0.5) & (er<=0.03))
       grp{i}='M'
      else
        grp{i}='A';
      end
```

IV. Results And Discussion

A. Simulation setup

To detect packet dropper selfish node with the help of behavior of nodes using a SVM classifier. We consider a typical deployment of sensor networks, where a number of sensor nodes are randomly deployed in a two dimensional area. Each sensor node generates sensory data periodically and all these nodes collaborate to forward packets containing the data towards a sink. The sink is located within the network. We assume all sensor nodes and the sink are loosely time synchronized which is required by many applications. For collecting network statistics simulation has been used under ns-3.14 in Ubuntu system. Proposed method uses the concept of behavior classification. For classification of nodes behavior Support Vector Machine (SVM) has been applied for achieving this MATLAB SVM has been used. Proposed approach performs fast and responds quickly to the packet dropper node.

Table 2: Simulation Parameter

Parameter	Value
Simulator	NS-3 (V NS-3.14)
Mobility Model	Random Waypoint model
Nodes (WifiNode's)	20, 30, 50,80, 100 nodes
Simulation Time	100s
Packet Size	1000 bytes
Update Interval	15s
Node Speed	10 m/s
Traffic Model	Constant Bit Rate
Traffic Type	UDP

Network simulation having two most important part first parameters required for network simulation and second the simulation of network scenario for performing the experiments and results evaluation

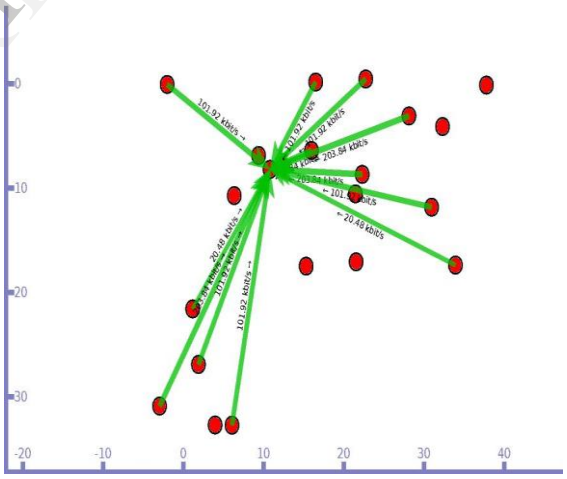

Fig. 1 WSN Simulation at time 20 sec

B. Result Analysis

Proposed behavior based anomaly detection techniques core concept is to make profile of each node and compare with the standard (normal) profile and check the deviation, if found i.e. attack has been detected. Proposed approach has considered the packet dropper/selfish node attack.

Proposed approach outperform well as compared to existing methods, following results has been obtained-

Figure 2 shows the number of packet lost in presence of Packet Dropper Nodes in WSN topology. Here x-axis represents the number of nodes and y-axis count the number of packets drop by node.

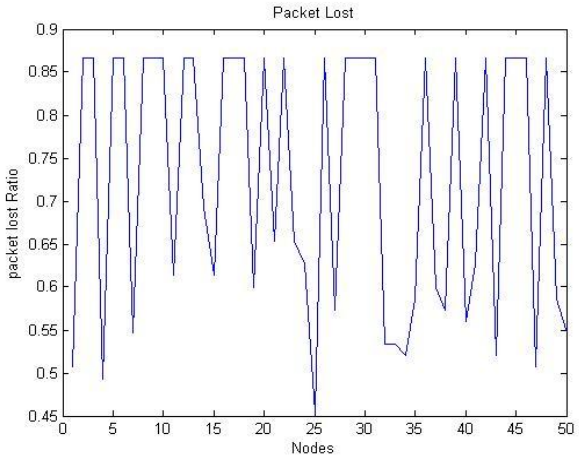

Fig. 2 Packet Lost in Presence of Packet Dropper Node

Whereas figure 3 shows the PDR ratio obtained in presence of packet dropper nodes, here x-axis represents the number of nodes and y-axis count the number of packets drop by nodes.

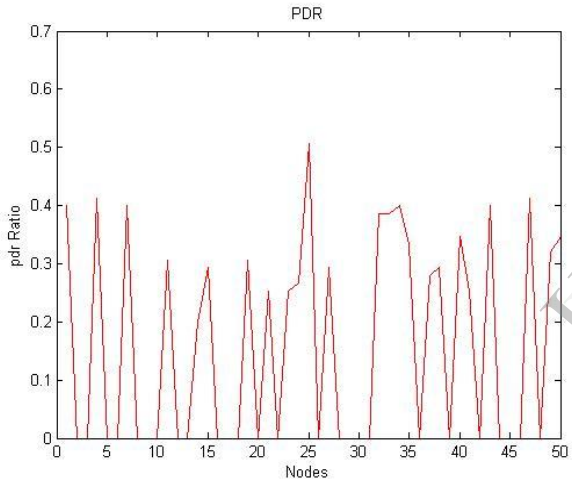

Fig. 3 Packet Delivery Ratio in Presence of Packet Dropper Node

Figure 4 shows the results obtained using propose approach. It caught the number packet Dropper node present in WSN simulating environment of 10 nodes. Here x-axis and y-axis is represents the classification of support vector machine (SVM) in which the range of metrics (pdr, pmir) 1 to 100% has been shown. The legend "a" having green lines represent the number of authentic node while "m" having red lines shows the number of Packet.

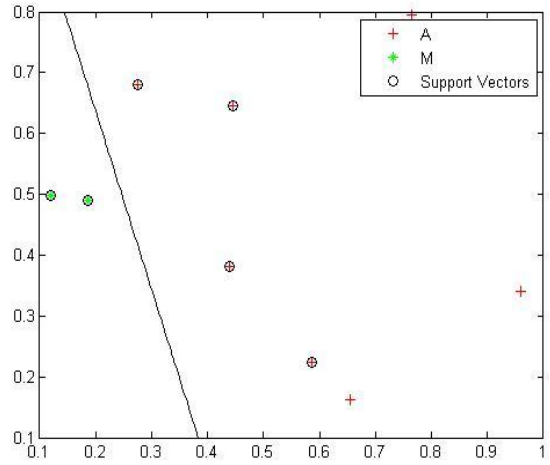

Fig. 4 Detection of Packet Dropper node using proposed behavior based method in Wireless Sensor Network

Figure 5 shows the detection rate of proposed method and existing method. Graph shows the number of rounds in X axis and in Y axis provides the detection ratio during experiments, where red line shows the performance of proposed algorithm and green line shows the existing method performance.

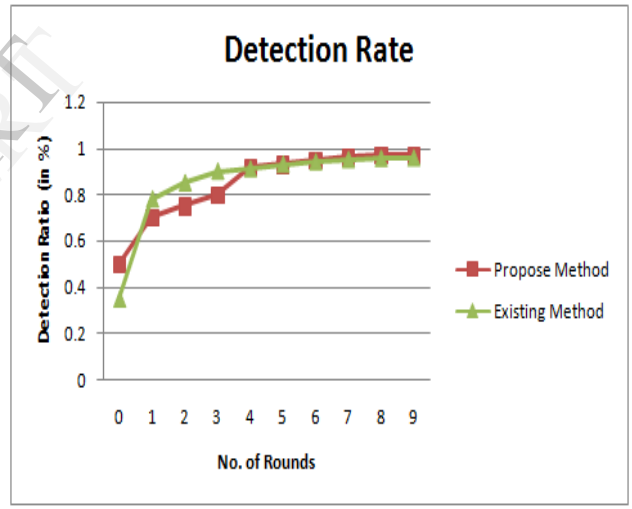

Fig. 5 Detection rate of proposed and existing method

V. CONCLUSION

Security threat and routing holes in wireless scenario are more frequent than other networks. Lack of infrastructure and centralized monitoring using limited battery power are the crucial point. Attackers can easily launch an attack to consumed resources of wireless network such as battery power packet dropping attack in sensor network.

In this proposed study work we have described various existing technique of WSN security to detect and prevent attacks like selfish node, black hole or packet droppers and modifiers (alternatively) with their strength and weakness. SVM is the novel concept in communication especially in the field of the security in wireless. We have proposed an anomaly based solution for the packet droppers and modifiers attack on WSN. Proposed algorithm has adopted the idea of machine learning technique in context of the anomaly detection to identify the attacks in the network. The idea has incenses from

the human society concept i.e. behavior of the node during communication. All the behaviors have been recorded distributive manner then machine learning has been applied to check the behavior of the node and consequently to detect packet dropping attacks.

The future of wireless sensor networks is really appealing, giving the vision of anytime, anywhere and cheap communications. Before those imagined scenarios come true, huge amount of work is to be done in both research and implementation. The study of the proposed work is completed yet and the performance evaluation is completed after that we found an anomaly based solution for the packet droppers and modifiers attack on WSN provide high performance QoS parameters and adoptable for use. In near future we stick with the same concept and work for more security issue.

ACKNOWLEDGMENTS

I am grateful to my Project Guide Dr. Sadhna K. Mishra whose guidance by we successfully completed our project. They willingly took the trouble of sparing his valuable time for our work and were always ready to help with his knowledge and valuable suggestions

REFERENCES

[1] Chuang Wang, Taiming Feng, Jinsook Kim, Guiling Wang and Wensheng Zhang "Catching Packet Droppers and Modifiers in Wireless Sensor Networks", IEEE Transactions On Parallel And Distributed Systems, Vol. 23, No. 5, May 2012.

[2] Vasaki Ponnusamy, Anang Hudaya and Alan G. Downe "A Biologically Inspired Energy Efficient Intrusion Detection System", IEEE, International Conference on Computer & Information Science (ICCIS), 2012.

[3] Krishna Doddapaneni, Enver Ever, Orhan Gemikonakli, Leonardo Mostarda and Alfredo Navarra "Effects of IDSs on the WSNs Lifetime: Evidence of the Need of New Approaches", IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications, 2012.

[4] Colin O'Reilly, Alex Gluhak, Muhammad Imran and Sutharshan Rajasegarar "Online Anomaly Rate Parameter Tracking for Anomaly Detection in Wireless Sensor Networks", 9th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON), 2012.

[5] Vlajic and N. Moniz, "Self-healing wireless sensor networks: Results that may surprise," In Globecom Workshops, Nov. 2007..

[6] Chris Karlof, David Wagner, "Secure Routing in Wireless Sensor Networks", Attacks and Countermeasures", Ad Hoc Networks (elsevier), Page: 299-302, 2003.