International Journal of Technology Research and Management
ISSN (Online): 2348-9006
Vol 1 Issue 2 May 2014

Behavioral based Anomaly Detection of Packet Drops in Wireless Sensor Network

Umesh Namdev
Department of Computer Science & Engineering, Shahdol Polytechnic College Shahdol
umesh.namdev@gmail.com

Abstract: - *Security threat and routing holes in wireless scenario are additional frequent than different networks. Lack of infrastructure and centralized watching exploitation limited battery power are the crucial purpose. Attackers can merely launch associate degree attack to consumed resources of wireless network like battery power packet dropping attack in device network. In such exploiting condition associate degree antagonist node may launch various attacks to disturb the communication in WSN. Amidst of such attacks packet dropping and modifier are the foremost prevailing attacks. In packet dropping attack compromising nods starts dropping each and each packet pass from him (node) or modify the packet before forwarding in a very later attack. In wireless device network, there are such a big amount of challenges and issues as already been mentioned and projected. The foremost challenges are how to offer most periods of time to network and also the way to supply hardiness to network. In device network, the energy is principally consumed for three purposes: data transmission, signal process, and hardware operation. Throughout this article we've Propose machine learning based mechanism to spot the routing holes on wireless device network. The conception lies on social behavior of the human society within that individual's behavior is that the benchmark to create your mind up his credibility within the network. Projected system works on the conception of the anomaly detection owing to unlabelled data manufacture by the device nodes. The target of this analysis article is to identify packet dropping and modifier in wireless device network against the set of qualitative performance metrics.*

Keywords: - *control Overhead, delivery ratio, energy remains, Machine learning, sensor, wireless sensor network, WSN, packet dropper.*

1. 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 furthermore as widely applied on wildlife tracking and then forth. Sensor nodes are one of the first elements that sense the scene and monitor it, observe the results, collection them to process the data and directed on the way to a sink node. In WSN another important entity is sink node which 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 wide deployed on inaccessible and in hostile habitat to observe and gather the data associated with that environment.

Security needs of WSN in such network due to lack of physical protection on it. The attacker will simply launch associate attack in such situation and disrupt

the communication. In such exploiting condition an antagonist node could 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 every and each packet pass from him (node) or modifies 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 below structure of wireless communication helps adversaries to perform variety of passive, active and stealth type of attacks easily. In passive mode, associate adversary or attacker wordlessly observe the radio channels so as to capture knowledge, gain security credentials, or to gather confidential information to derive the credentials. In active attacks, adversaries could pay attention to the network transmissions, capture and read the contents of data packets send by sensor nodes. A protection scheme detects the various type of attacks and sends the report back to base station or all nodes in network. It uses all nodes or some special nodes to observe these types of attacks. These nodes co-operate one another to require the decision and at last send the report back to the base station. It needs lots of communication between the nodes. If adversary will trap the message exchanging between the nodes then they'll simply tamper the messages and send the false data to the other nodes.

In wireless sensor network, there are such a big amount of challenges and problems as already been mentioned and projected. The main challenges are the way to provide most lifetimes to network and the way to supply robustness to network. In sensor network, the energy is principally consumed for 3 purposes: data transmission, signal processing, and hardware operation. It's said in [5] that 70th of energy consumption is because of data transmission.

In packet dropping attack compromising nods starts dropping every and each packet pass from him (node) or modifies the packet before forwarding. Propose a machine learning based mechanism to identify the routing holes on wireless sensor network. The idea lies on social behavior of the human society in which individual's behavior is that the benchmark to make your mind up his authenticity within the network. Proposed system works on the concept of the anomaly detection because of unlabeled information produce by the device nodes. The overall objective of this analysis article is to spot packet dropper and modifier in wireless device network against the set of qualitative performance metrics.

The specific goals of this analysis work:

- Determine the intrusion on the basis of the node energy remain as a metric.

- To extends the limitation of standard 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 knowledge should classify properly. Soft computing and learning methods produces the foremost 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 two describes related terminology and background work, and section three focuses on related work in WiMax area. Section four discusses the proposed solution; finally section five provides the conclusion of this paper.

2. RELATED WORK AND PROBLEM IDENTIFICATION

Before presenting the proposed methodology initial we wish to address the problem in existing system –

Problem has been identified in [1]:

a. Author has proposed a good approach however it restricts to DAG topology.

b. Author has used the concept of key exchange which appears computation overhead in such a battery constraint surroundings.

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 analysis are on self Healing i.e. energy utilization just 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 create WSN nodes as a self healing entity whereas there's battery drainage.

Problem Identified:

Author has used the concept of mobile agent that is good but restricted to the particular areas like remote station wherever monitoring is complex and infeasible like ever-changing the battery power.

Mobile agents are a good thought as a result of their autonomous (self executable) and social in nature however their management and security is that the larger challenge.

Problem has been identified in [3]:

Instead of proposing a new mechanism there's also a evaluation is needed to analyze the impact of the prevailing method with some common metrics, author [3] has do the same within the article in which existing IDS techniques (whether they are anomaly based or signature one) has been chosen to check 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 that.

Author has used the idea of SVM for detecting attacks in WSN. We've got chosen author idea for improvement in the research areas.

Proposed system can design to detect and prevent packet dropper nodes within the WSN. Proposed scheme is that the enhancement of the author's [1] and [4] technique.

In this paper some a lot of metrics are going to be required to reinforce SVM based mostly classifier mechanism that we'll discuss in our proposed mechanism.

Author has applied the proposed behavior based mostly mechanism on sink node, however our technique has been applied to every node which reduces the procedure overhead.

Proposed system can think about 2 types of attack that is more associated with packet dropper attack.

i. Selfish Node

ii. Black Hole

3. PROPOSED ALGORITHM

In wireless sensor network scenario the greatest problem that has been seen now a days may be a security threat like packet dropper attack resulting the battery consumption and finally disrupting the sensor networks working. Proposed method's core idea is anomaly detection technique of IDS during which the deviated profile are going to be treated as anomaly. For the base profile the conventional transmission profile of the node are going to be chosen throughout packet transmission.

The general idea of the proposed works as follow-

To enhance the performance of the higher than mentioned scheme we've got integrated the thought of classification of the behavior of selfishness and black hole nature using support vector machine.

Nodes are planned to expand the most reimbursement from the networks when safeguard their own resources like hardware, battery power or bandwidth. Selfish nodes do only outgoing from their own. Thence they only send information packets to alternative node as a source. While once receiving packets from alternative nodes they refused to cooperate. Consequently, they begin dropping of packets or refuse.

Proposed solution is predicated 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 traditional profile of Nodes during communication based on their behavior with facilitate 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 subsequent proposed methodology we've got develop to limit the selfishness of a node in wireless infrastructure less environment –

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

ii. Applying the threshold mechanism on every node to restrict the flooding of reserve route management packets within the network (Using observation pr supervision of behavior) with help of support vector machine (SVM).

Same mechanism will apply to sight black hole attack and inflicting node for constant. The most concern property in black hole is going to be the response of packet delivery ratio (Packet_Del_R) of the node. Proposed solution is predicated on anomaly detection concept of Intrusion Detection System. During this proposed technique the behavioral (during transmission) metrics of the sensor nodes works as an anomaly benchmark. Hence behavioral data has been wont 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 higher resolution that is economical, scalable, energy saving and robust–

1. Building behavioral profile of Nodes whereas communicating in sensor surroundings. Because it knows that anomaly detection approach requires one benchmark profile i.e. traditional profile to compares while detecting the attacks. For this 1st proposed system has build traditional profile of sensor nodes using simulation. For this activity of the nodes has been collected from the simulation environment of traditional condition. Later on 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 create traditional 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. begin the Simulation and build the record the transmission information i.e. of activity profile of the sensor nodes.

c. Collect the activity statistics into .xml or .tr (trace) file format and also record the routing overhead and number of hello messages of every node

d. Parse .xml file to work out the metrics associated with sensing nodes using scilab or weka to

e. confirm the value of Pkt_Del_R, RO , No_Hello_msg and ER and for every node (Note: the value of ER and No_Hello_msg has been extracted using test files generated throughout 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 higher understanding the traditional and attack has been labeled as “d” for „dropper‟ and “a” for „authenticate‟ node in support Vector Machine (SVM).

Algorithm to classify the sensor nodes:-

Algorithm II: Behavioral Classification to Detect Packet Dropper

```
nmp={}; // Array variable to store packet dropper

for j=1:node

if(pkt_del_r(j)>=0.7)

nmp {j}='A' //authenticated Node

elseif((pkt_del_r (j)>=0.5 & pmir(j)>=0.3))

nmp ji}='M' //paket Dropper

elseif(((pdr(j)<0.5 &pmir(j)>=0.5)||pmir(j)>=0.7)

nmp {j}='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
```

4. RESULTS AND DISCUSSION

4.1 Simulation Setup

To detect packet dropper selfish node with the help of behavior of nodes employing a SVM classifier. We tend to think about a typical deployment of sensor networks, wherever varieties of sensor nodes are arbitrarily deployed in a 2 dimensional area. Every sensor node generates sensory information periodically and all these nodes collaborate to forward packets containing the information towards a sink. The sink is found within the network. We tend to assume all sensor nodes and therefore the sink are loosely time synchronous that is needed by many applications. For collecting network statistics simulation has been used under ns-3.14 in Ubuntu system. Proposed methodology 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.

Network simulation having 2 most vital part first parameters needed for network simulation and second the simulation of network scenario for playing the experiments and results analysis.

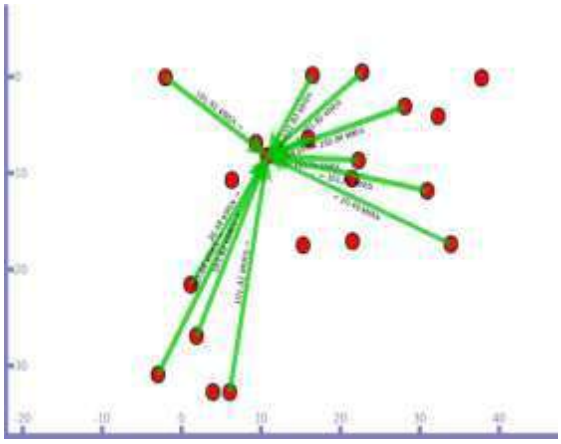

Fig. 1 WSN Simulation at time 20 sec

Proposed behavior based anomaly detection techniques core concept is to create profile of every 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 amount of packets drop by node.

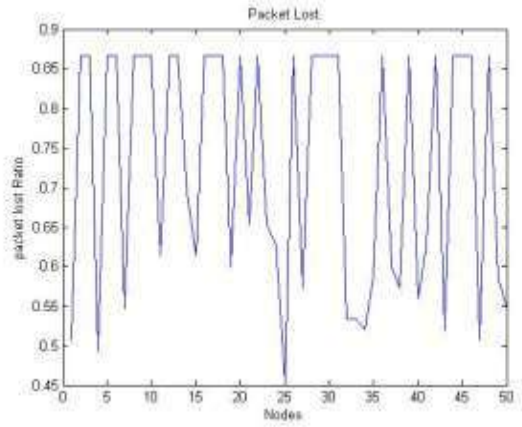

Fig. 2 Packet Lost in Presence of Packet Dropper Node

Whereas figure three 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.

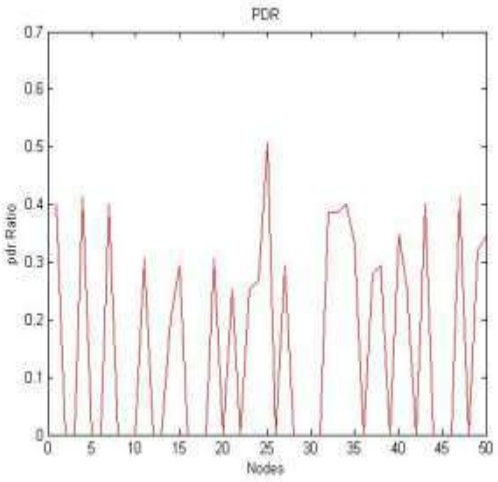

Fig. 3 Packet Delivery Ratio in Presence of Packet Dropper Node

Figure four shows the results obtained using propose approach. It caught the number packet dropper node present in WSN simulating setting of ten nodes. Here x-axis and y-axis is represents the classification of support vector machine (SVM) within which the range of metrics (pdr, pmir) one to 100 percent 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.

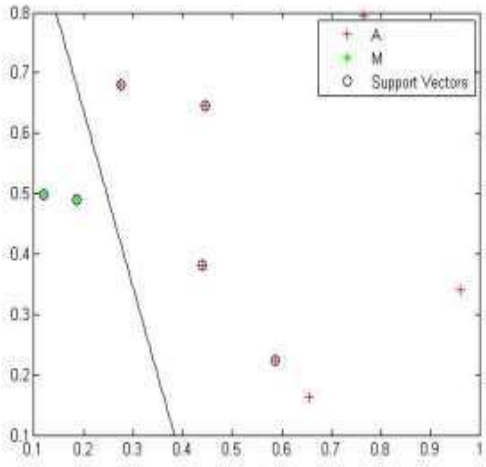

Fig. 4 Detection of Packet Dropper node using proposed behavior based method in Wireless Sensor Network

Figure five shows the detection rate of proposed methodology and existing methodology. Graph shows the number of rounds in X axis and in Y axis provides the detection ratio throughout experiments, wherever red line shows the performance of proposed algorithm and green line shows the present method performance.

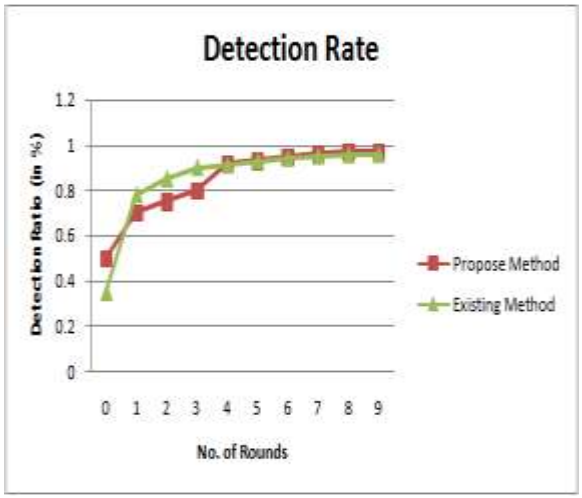

Fig. 5 Detection rate of proposed and existing method

5. CONCLUSION

Security threat and routing holes in wireless scenario are more frequent than other networks. Lack of infrastructure and centralized monitoring using restricted battery power are the crucial purpose. Attackers will simply launch an attack to consumed resources of wireless network like battery power packet dropping attack in sensor network.

In this proposed study work we've represented numerous existing technique of WSN security to discover and prevent attacks like selfish node, black hole or packet droppers and modifiers (alternatively) with their strength and weakness. SVM is that the novel thought in communication particularly in the field of the security in wireless. We've 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 within the network. The idea has incenses from the human society thought i.e. behavior of the node throughout communication. All the behaviors are recorded distributive manner then machine learning has been applied to check the behavior of the node and consequently to discover packet dropping attacks.

The future of wireless sensor networks is really appealing, giving the vision of anytime, anywhere and cheap communications. Before those notional scenarios come true, huge quantity of work is to be tired each analysis and implementation. The study of the proposed work is completed yet and the performance analysis is completed after that we tend to found an anomaly based solution for the packet droppers and modifiers attack on WSN provide high performance QoS parameters and adoptable to be used. In near future we tend to stick to the same thought and work for additional security issue.

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.