ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Issue 11, November 2016

Efficiently Detection of Selective Forwarding Attacks and Reduction of Overhead by using CBI method in WSN

D.Regi Timna, R.JothiRaj, Immanuel Vinoth.P,Assistant Professor
Department of Electronics and Communication Engineering
Francis Xavier Engineering College, Tirunelveli, India.

R.K.Shunmuga Priya,PG Student
Department of Electronics and Communication Engineering
Francis Xavier Engineering College, Tirunelveli, India.

Abstract: The wireless sensor network has become an important area and it is widely applied to military and civilian applications. These are easily prone to security attacks because it handling wireless media for transmission. Without any convenient security solution, the malicious node will act as a normal node in the network which causes eaves dropping and selective forwarding attack. A malicious nodes behaves like black hole and may refuse to leading positive messages and easily trace them, assuring that they are not all propagated any further in this attacks. However, such an attacker runs the dangers that neighboring nodes will conclude that it has failed and decide to seek another route. Most of the existing studies on selective forwarding attacks target on attack detection under the assumption of an error-free wireless channel. This proposed method analyze the attack using a more practical and challenging scenario that packet dropping may be due to an expected attack, or normal loss events such as medium access collision or bad channel quality. A Channel Based Identification (CBI) method is developed that can efficiently identify the selective forwarding misbehavior from the normal losses. A CBI method has two different strategies, Channel Identification (CI) and Data Traffic Identification (DTI). If data loss rate at certain nodes exceeds over the estimated normal loss rate, those nodes used for communication will be marked as attackers.

Keywords: Wireless Sensor Network, Selective Forwarding Attack, CBI, CI, DTI

I. Introduction

In today's fast and promptly growing world of technologies, more and more businesses understand the advantages of usage of computer networking. Depending on the firm's size and resources it might be a small LAN which incorporates only a few dozen computers; however in large enterprise the networks can grow to enormous and complex mixture of computers and servers. A computer network is a structure for communication between computers. These networks may be fixed (cabled, permanent) or temporary (as via modems/null modems). The researchers and businesses to families and individuals in everyday use increases numbers and types of users of networks. Since their evolution in the 1970s; wireless networks have become increasingly trendy in the computing industry. This is particularly true within the past decade which has seen wireless networks being suited to enable mobility. There are two variations of mobile wireless networks currently. The first is known as infrastructure networks, i.e., those networks with fixed and wired gateways. The bridges are known as base stations. While the mobile travels out of range from one base station into the range of another, a "handoff" occurs and the mobile continues communication throughout the network. All nodes can be connected dynamically in a random manner. Nodes discover and maintain routes to other nodes as the function of routers in the network.

In the attempt to upgrade the system performance of wireless networks, network coding has been shown to be an effective and encouraging approach and it is compared to conventional networks, where intermediate nodes store and forward packets as the original. The forwarders are allowed to receive and apply encoding schemes, thus they create and transmit new packets. These coding systems face new challenges and attacks, whose impact and remedy are still not well understood because their hidden characteristics are different from well-studied conventional wireless networks. The selective forwarding attack is one of these attacks. The attacker can forward each packet using selective forwarding links and without modifies the packet transmission by routing it to an unauthorized remote node in this attack. Hence, receiving the rebroadcast packets by the attackers, a few nodes will have the confusion that they are close to the attacker. With the ability of dynamic network topology and bypassing packets for further manipulation, selective forwarding attackers pose a severe threat to many functions in the network, such as routing and localization. To investigate this attack in wireless network coding systems, focus on their impact and countermeasures in a class of popular network coding scheme - Random Linear Network Coding (RLNC) system.

This attacks cause serious disruption to network functions and downgrade system performance and also severely compromise the network coding protocols. In particular, if they are launched in routing, the nodes which are close to attackers will receive more packets than they should and be treated as having a good efficiency for forwarding packets. Thus they will be assigned with more obligations in packet forwarding than what they can actually provide. This unfair distribution of workload will result in inefficient resource utilization and diminish the system performance. Firstly, selective forwarding attacks become more sophisticated attacks, such as man-in-the-middle attacks and entropy attacks. Secondly, the attackers can systematically turn on and off the links in data transmissions, complicated the system with fake link condition changes and making it unnecessarily rerun the routing process.

Some of the works under selective forwarding attack are Ju Ren, Y. Zhang, K.Zhang and X.Shen [1] proposed Channel-Aware Reputation System with Adaptive Detection Threshold (CRS-A) & Attack-Tolerant Data Forwarding Scheme is developed. Improve more than 10% data delivery ratio for the network. Suat Ozdemir [2] proposed a Reliable Data Aggregation and Transmission protocol and Reed-Solomon Coding scheme which improves Reliability, Secure, Efficient, Communication overhead and achieves DDR up to 30%. X.Lin, X.Liang, X.Shen [3] proposed a Trust Based Encryption (TBE), basic TSE (bTSE) & Sybil-resisted TSE (SrTSE) scheme are used. SrTSE detects Sybil attacks; bTSE achieves better performance in terms of rate & delay. The bTSE achieves 100% efficiency can effectively resist the review rejection attack. Sophia Kaplantzis et al. [4] proposed a Support Vector Machines (SVMs), Minimum Transmission Energy (MTE) and sliding windows technique use a simple classification based IDS (Intrusion Detection System) to detect this attack in WSN. This scheme based on the 2D feature vector (bandwidth, hop count), the alarms are raised. proposed a scheme which uses a multi-hop acknowledgment scheme to launch alarms by obtaining responses from intermediate nodes by detecting whether a node as malicious in its downstream/upstream[8].

The main objective of this paper is to detect and localize selective forwarding attacks in wireless network coding systems. The major differences in routing and packet forwarding rule out using existing countermeasures in conventional networks. The connectivity in the network is described using the link loss probability value between each pair of nodes, while common networks use connectivity graphs with a binary relationship (i.e., connected or not) on the set of nodes. Some more existing works rely on the packet round trip time difference introduced by selective forwarding attacks to detect them. Unfortunately, this type of solutions cannot work with network coding. They require either to use a traditional route that does not exist with network coding, or to calculate the delay between every two neighboring nodes which will introduce a huge amount of error in network coding systems.

The rest of the paper is organized as follows. Proposed method and algorithms are explained in section II. Results and discussion are presented in section III. Conclusion are given in section IV.

II. Proposed Method

In the Existing System, a Channel-Aware Reputation System with Adaptive Detection Threshold (CRS-A) was developed to detect selective forwarding attacks in WSN. To distinguish selective forwarding attacks from the normal packet loss derived from the optimal evaluation threshold of CRS-A in the probabilistic way, which is adaptive to the time-varied channel condition and attack probabilities of compromised nodes. Each sensor node maintains a reputation table to evaluate the long-term forwarding behaviours of its neighbouring nodes. Once the reputation value of a senor node is below an alarm value, it would be identified as a normal node. Rather than isolating all the compromised nodes from data forwarding, it jointly considers the time-varied channel condition and attack probabilities of neighbouring nodes in choosing forwarding nodes. Detection of this attacks becomes more challenging, if the normal packet loss rate is more fluctuant and difficult to estimate due to the mobility of sensor nodes. This cannot identify the exactly node is misbehaving node using reputation table, Data access delay is more and high communication overhead are the problems in existing system

A. Selective Forwarding Attack Detection

In this paper Channel Based Identification (CBI) method can identify the selective forwarding attackers by filtering out the normal channel losses. The Channel Identification (CI) is integrated with Data Traffic Identification (DTI) to achieve channel-aware detection of selective forwarding misbehaviour hidden in the normal loss events due to bad channel quality or MAC. Estimation of packet loss due to wireless channel quality, termed as wireless loss probability, by modelling the underlying time varying wireless channel. In CBI, attack detection is based on the combination of downstream and upstream monitoring. The downstream/upstream monitoring opinions are configured by comparing the loss rates with the downstream/upstream detection thresholds. Due to the randomness nature, even without selective forwarding attack, a burst of normal loss events in certain situations may lead to the false alarm. A false clear or missed detection occurs when the detection scheme does not give an alarm but a threat exists. Also concluded that both upstream and downstream monitoring is necessary for accurately detecting the attackers.

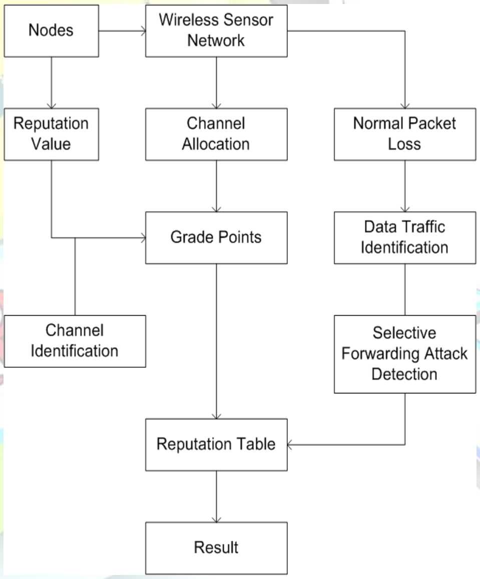


Fig.1Block diagram

Fig 1 describes that for every data transmission starts, the routing manager assures that the node is a trusted node or not. Based on the threshold value the node trust is decided. Every node has a specific threshold value. The threshold value is calculated based on the nodes present in the network. If the threshold value is in range then the node is moved to the Node list. If the threshold value is in out of range then the node is moved to the black list. If the threshold value of the node is not justified then it is moved to the warning list. The trust node is present only in the node list. After the trust nodes are identified then the nodes are monitored by network monitor and add to the member list. The member list nodes are only allowed for data aggregation. The collection of data's are named as data units. The data's are collected from the cluster to the cluster head. This process is also monitored by routing manager. After complete this process the data aggregation starts securely and efficiently.

B. Channel Based Identification

In CBI module, each node maintains a history of packet counts such as how many packets it receives and overhears from its upstream and downstream node which are forwarded. Each node maintains a probability of distrust for its downstream node. The main advantages is that each node's behaviour in the path is observed by its upstream and downstream neighbours, and the thresholds are dynamically adjusted with the normal loss rates to maintain the detection accuracy when network status changes. This algorithm is difficult that extra packets are transmitted to detect the attack and also downstream traffic monitoring increase the traffic overhead.

C. Deploy The Trust Based Schemes

Nodes are going to create a list known as true list. In this they are going to store about the node information's which given proper response to the certificate authority. The utility of a sensor network will rely on its ability to accurately and automatically locate each sensor in the network. It is designed to locate faults will need accurate location information. Unfortunately, an attacker can easily employ non secured location information by reporting fake signal strengths and replaying signals. A node will send route request to other nodes whenever they want to send the data. The node which received the route request packet will check whether that node is present in the true list or not. Node will forward packets to other nodes and it will repeat until it reaches destination if it is in true list. Route trust is computed by every node in its routing table for each route. It is a measure of the reliability with which a packet can reach the destination, if forwarded by the node on that particular route. For every transmission starts before it check the route whether it is a trust list or hacking list. If it is a trust list then the data aggregation is done securely. When a Source Node the packet n times and drops the packet m times, the trust calculation will assign trust value

$$Trust = (n * [n + m/NeighborCount])$$

n = reputation value received from judge node.

The advantages of proposed system are to minimize the false alarm and missed detection probabilities & also PDR is improved. Do not rely on any location information, global synchronization assumption or special hardware/middleware and it depend on the local information only. Proposed solution also used in scenario where no central administration node exists. The centralized algorithm concentrates the computation workload to the central node, and thus each normal node will suffer much less workload. The communication overheads of the centralized algorithm are lower. Thus it can detect the selective forwarding link efficiently, and the resulted warnings can be delivered to each node more quickly.

Pseudo code to find the trust value for node against selective forwarding attack

```
1. repeat

RUSHING (M);

until all misbehaving, nodes are trusted nodes.

2.if (DropCount >= Average(NodeDropCount)) &&
(Average(NodeDropCount) < Sum(NodeDropCount))

then

Mark Selected node as attacker

else

if (SimulationTime >= 60ms)
```

```
 then
set Trust of Node
end if;
end if;
3.Stop.
```

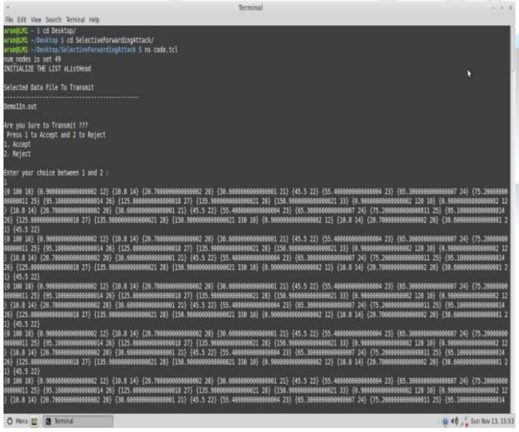
Techniques

The aim is to verify the behavior of known or unknown attacks. Behavioral detection include various headers such as source/ destination address of attacker or nodes, types of process and other statistical features. And each of the above technique can be further applied using static and dynamic analysis or hybrid analysis.

Algorithm: Naive Bayes

The next classifiers we are using a Naive Bayes classifier. It calculates the likelihood that a program is having malevolent code given the features that are present in the program. This approach used both string and byte sequences data for computing a probability of a binary's malicious code having some features. The main assumption is that the binaries contain same features such as signatures and machine instructions.

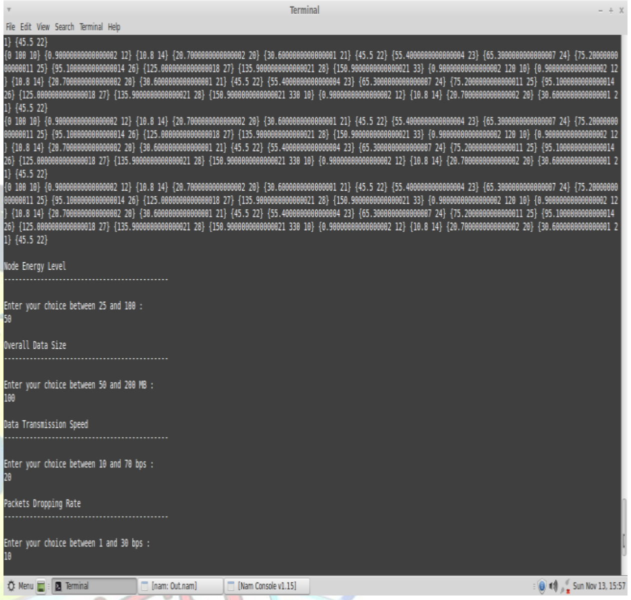
III.Results And Discussion



```
arun@LM1 ~ $ cd Desktop/
arun@LM1 ~/Desktop $ cd SelectiveForwardingAttack/
arun@LM1 ~/Desktop/SelectiveForwardingAttack $ ns code.tcl
num nodes is set 49
INITIALIZE THE LIST xListHead

Selected Data File To Transmit
---------------------------------------------
DemoIIn.out

Are you Sure to Transmit ???
 Press 1 to Accept and 2 to Reject
1. Accept
2. Reject

Enter your choice between 1 and 2 :
1
{0 100 10} {0.9000000000000002 12} {10.8 14} {20.700000000000002 20} {30.600000000000001 21} {45.5 22} {55.400000000000004 23} {65.300000000000007 24} {75.20000000
00000011 25} {95.100000000000014 26} {125.000000000000018 27} {135.900000000000021 28} {150.900000000000021 33} {0.9000000000000002 120 10} {0.9000000000000002 12
} {10.8 14} {20.700000000000002 20} {30.600000000000001 21} {45.5 22} {55.400000000000004 23} {65.300000000000007 24} {75.200000000000011 25} {95.100000000000014
26} {125.000000000000018 27} {135.900000000000021 28} {150.900000000000021 330 10} {0.9000000000000002 12} {10.8 14} {20.700000000000002 20} {30.600000000000001 2
1} {45.5 22}
{0 100 10} {0.9000000000000002 12} {10.8 14} {20.700000000000002 20} {30.600000000000001 21} {45.5 22} {55.400000000000004 23} {65.300000000000007 24} {75.20000000
00000011 25} {95.100000000000014 26} {125.000000000000018 27} {135.900000000000021 28} {150.900000000000021 33} {0.9000000000000002 120 10} {0.9000000000000002 12
} {10.8 14} {20.700000000000002 20} {30.600000000000001 21} {45.5 22} {55.400000000000004 23} {65.300000000000007 24} {75.200000000000011 25} {95.100000000000014
26} {125.000000000000018 27} {135.900000000000021 28} {150.900000000000021 330 10} {0.9000000000000002 12} {10.8 14} {20.700000000000002 20} {30.600000000000001 2
1} {45.5 22}
{0 100 10} {0.9000000000000002 12} {10.8 14} {20.700000000000002 20} {30.600000000000001 21} {45.5 22} {55.400000000000004 23} {65.300000000000007 24} {75.20000000
00000011 25} {95.100000000000014 26} {125.000000000000018 27} {135.900000000000021 28} {150.900000000000021 33} {0.9000000000000002 120 10} {0.9000000000000002 12
} {10.8 14} {20.700000000000002 20} {30.600000000000001 21} {45.5 22} {55.400000000000004 23} {65.300000000000007 24} {75.200000000000011 25} {95.100000000000014
26} {125.000000000000018 27} {135.900000000000021 28} {150.900000000000021 330 10} {0.9000000000000002 12} {10.8 14} {20.700000000000002 20} {30.600000000000001 2
1} {45.5 22}
{0 100 10} {0.9000000000000002 12} {10.8 14} {20.700000000000002 20} {30.600000000000001 21} {45.5 22} {55.400000000000004 23} {65.300000000000007 24} {75.20000000
00000011 25} {95.100000000000014 26} {125.000000000000018 27} {135.900000000000021 28} {150.900000000000021 33} {0.9000000000000002 120 10} {0.9000000000000002 12
} {10.8 14} {20.700000000000002 20} {30.600000000000001 21} {45.5 22} {55.400000000000004 23} {65.300000000000007 24} {75.200000000000011 25} {95.100000000000014
26} {125.000000000000018 27} {135.900000000000021 28} {150.900000000000021 330 10} {0.9000000000000002 12} {10.8 14} {20.700000000000002 20} {30.600000000000001 2
1} {45.5 22}
{0 100 10} {0.9000000000000002 12} {10.8 14} {20.700000000000002 20} {30.600000000000001 21} {45.5 22} {55.400000000000004 23} {65.300000000000007 24} {75.20000000
00000011 25} {95.100000000000014 26} {125.000000000000018 27} {135.900000000000021 28} {150.900000000000021 33} {0.9000000000000002 120 10} {0.9000000000000002 12
} {10.8 14} {20.700000000000002 20} {30.600000000000001 21} {45.5 22} {55.400000000000004 23} {65.300000000000007 24} {75.200000000000011 25} {95.100000000000014
```

Fig 2 Initialization of Input

Fig 2 explains about the input setting as numbers of nodes is 49 and selects the data file which has to be transmitted and also confirm the file that has been sure to transmit.



```
1} {45.5 22}
{0 100 10} {0.9000000000000002 12} {10.8 14} {20.700000000000002 20} {30.600000000000001 21} {45.5 22} {55.400000000000004 23} {65.300000000000007 24} {75.20000000
00000011 25} {95.100000000000014 26} {125.000000000000018 27} {135.900000000000021 28} {150.900000000000021 33} {0.9000000000000002 120 10} {0.9000000000000002 12
} {10.8 14} {20.700000000000002 20} {30.600000000000001 21} {45.5 22} {55.400000000000004 23} {65.300000000000007 24} {75.200000000000011 25} {95.100000000000014
26} {125.000000000000018 27} {135.900000000000021 28} {150.900000000000021 330 10} {0.9000000000000002 12} {10.8 14} {20.700000000000002 20} {30.600000000000001 2
1} {45.5 22}
{0 100 10} {0.9000000000000002 12} {10.8 14} {20.700000000000002 20} {30.600000000000001 21} {45.5 22} {55.400000000000004 23} {65.300000000000007 24} {75.20000000
00000011 25} {95.100000000000014 26} {125.000000000000018 27} {135.900000000000021 28} {150.900000000000021 33} {0.9000000000000002 120 10} {0.9000000000000002 12
} {10.8 14} {20.700000000000002 20} {30.600000000000001 21} {45.5 22} {55.400000000000004 23} {65.300000000000007 24} {75.200000000000011 25} {95.100000000000014
26} {125.000000000000018 27} {135.900000000000021 28} {150.900000000000021 330 10} {0.9000000000000002 12} {10.8 14} {20.700000000000002 20} {30.600000000000001 2
1} {45.5 22}
{0 100 10} {0.9000000000000002 12} {10.8 14} {20.700000000000002 20} {30.600000000000001 21} {45.5 22} {55.400000000000004 23} {65.300000000000007 24} {75.20000000
00000011 25} {95.100000000000014 26} {125.000000000000018 27} {135.900000000000021 28} {150.900000000000021 33} {0.9000000000000002 120 10} {0.9000000000000002 12
} {10.8 14} {20.700000000000002 20} {30.600000000000001 21} {45.5 22} {55.400000000000004 23} {65.300000000000007 24} {75.200000000000011 25} {95.100000000000014
26} {125.000000000000018 27} {135.900000000000021 28} {150.900000000000021 330 10} {0.9000000000000002 12} {10.8 14} {20.700000000000002 20} {30.600000000000001 2
1} {45.5 22}

Node Energy Level
---------------------------------------------


Enter your choice between 25 and 100 :
50

Overall Data Size
---------------------------------------------


Enter your choice between 50 and 200 MB :
100

Data Transmission Speed
---------------------------------------------


Enter your choice between 10 and 70 bps :
20

Packets Dropping Rate
---------------------------------------------


Enter your choice between 1 and 30 bps :
10
```

Fig 3 Parameter Initialization

Fig 3 shows the initial parameter setting such as Node Energy Level, Overall Data Size, Data Transmission Speed and Packets Dropping Rate by user.

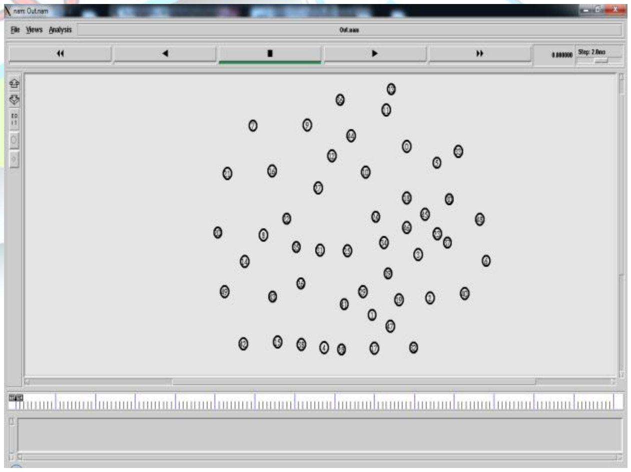
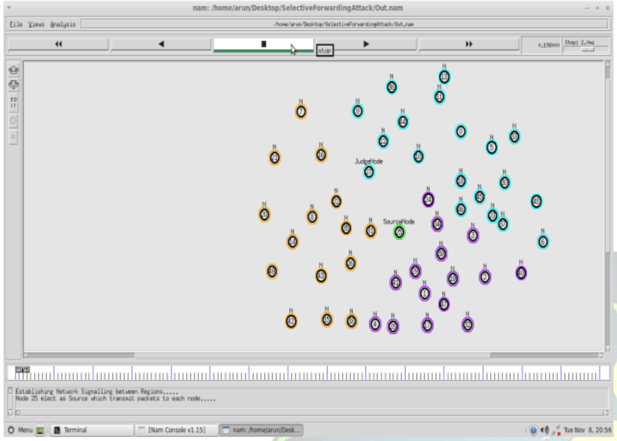


Fig 4 Initialization of Nodes

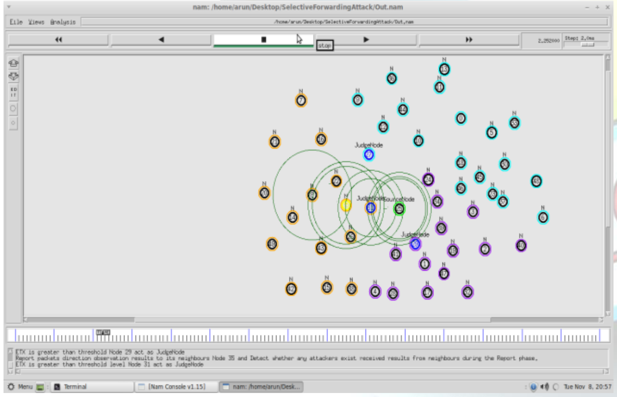
Fig 4 shows the setting of 49 nodes from 0 to 48 and that are initialized.



```
Establishing Network Signalling between Regions.....
Node 25 elect as Source which transmit packets to each node.....
```

Fig 5 Division of Nodes

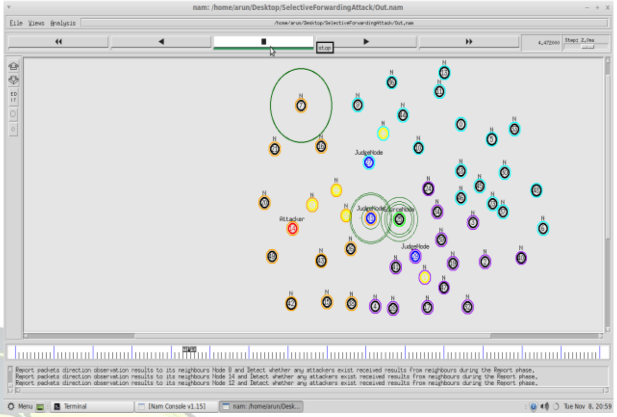
The above figure set the 25th node as Source Node and it is represented as Green colour. Nodes are divided into 3 Regions with orange, blue and purple colors.



```
ETX is greater than threshold Node 29 act as JudgeNode
Report packets direction observation results to its neighbours Node 35 and Detect whether any attackers exist received results from neighbours during the Report phase.
ETX is greater than threshold level Node 31 act as JudgeNode
```

Fig 6 Set Judge Nodes

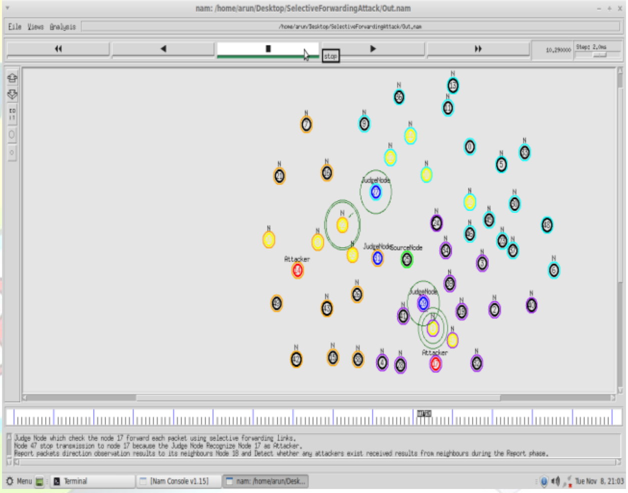
Fig 6 shows that the Judge Node setting for each regions and then starts the communication between nodes.



```
Report packets direction observation results to its neighbours Node 8 and Detect whether any attackers exist received results from neighbours during the Report phase.
Report packets direction observation results to its neighbours Node 14 and Detect whether any attackers exist received results from neighbours during the Report phase.
Report packets direction observation results to its neighbours Node 12 and Detect whether any attackers exist received results from neighbours during the Report phase.
```

Fig 7 Attackers Detection in I Region

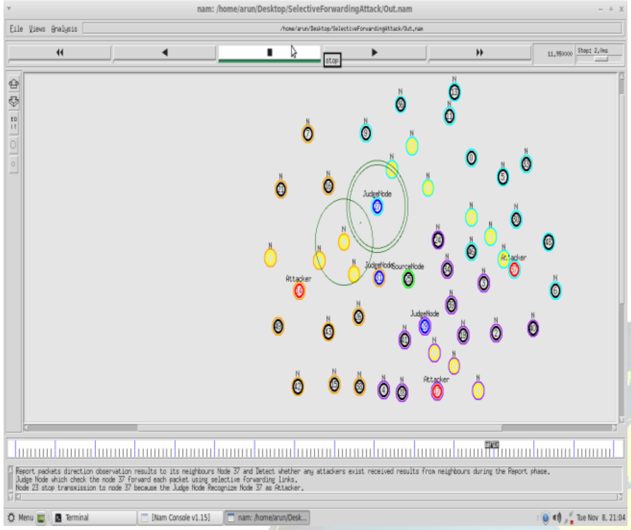
Fig 7 shows that the Attackers in 14th node are detected in 1st region which drop the packets.



```
Judge Node which check the node 17 forward each packet using selective forwarding links.
Node 47 stop transmission to node 17 because the Judge Node Recognize Node 17 as Attacker.
Report packets direction observation results to its neighbours Node 18 and Detect whether any attackers exist received results from neighbours during the Report phase.
```

Fig 8 Attackers Detection in II Region

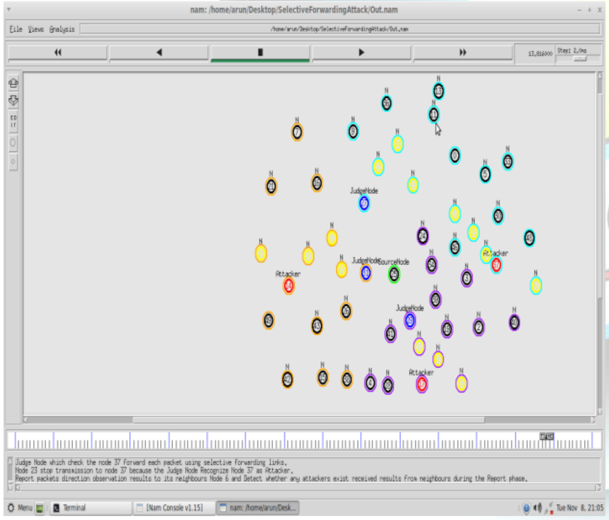
Fig 8 shows that the 17th node is attackers in 2nd region & JN share others to stop communicate with them.



```
Report packets direction observation results to its neighbours Node 37 and Detect whether any attackers exist received results from neighbours during the Report phase.
Judge Node which check the node 37 forward each packet using selective forwarding links.
Node 23 stop transmission to node 37 because the Judge Node Recognize Node 37 as Attacker.
```

Fig 9 Attackers Detection in III Region

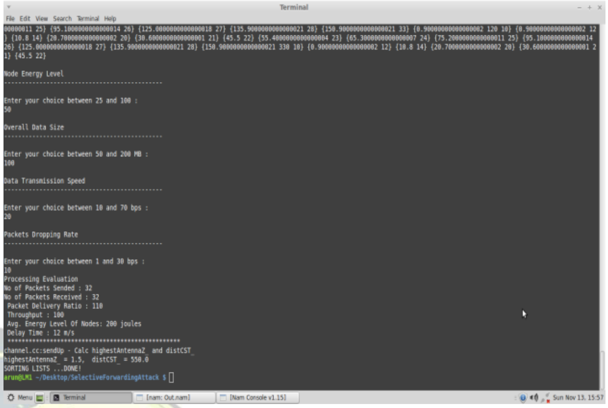
Fig 9 explains about the 37th node is attackers in 3rd region and all the attackers are denoted as Red color.



```
Judge Node which check the node 37 forward each packet using selective forwarding links.
Node 23 stop transmission to node 37 because the Judge Node Recognize Node 37 as Attacker.
Report packets direction observation results to its neighbours Node 6 and Detect whether any attackers exist received results from neighbours during the Report phase.
```

Fig 10 Final Output

Fig 10 shows that the all the attackers are detected & the remaining nodes shares transmission b/w them without any attackers finally.



```
00000011 25} {95.10000000000000014 26} {125.00000000000000018 27} {135.90000000000000021 28} {150.90000000000000021 33} {0.90000000000000002 120 10} {0.90000000000000002 12
} {10.8 14} {20.70000000000000002 20} {30.60000000000000001 21} {45.5 22} {55.40000000000000004 23} {65.30000000000000007 24} {75.20000000000000011 25} {95.10000000000000014
26} {125.00000000000000018 27} {135.90000000000000021 28} {150.90000000000000021 330 10} {0.90000000000000002 12} {10.8 14} {20.70000000000000002 20} {30.60000000000000001 2
1} {45.5 22}

Node Energy Level
--------------------------------------------


Enter your choice between 25 and 100 :
50

Overall Data Size
--------------------------------------------


Enter your choice between 50 and 200 MB :
100

Data Transmission Speed
--------------------------------------------


Enter your choice between 10 and 70 bps :
20

Packets Dropping Rate
--------------------------------------------


Enter your choice between 1 and 30 bps :
10
Processing Evaluation
No of Packets Sended : 32
No of Packets Received : 32
 Packet Delivery Ratio : 110
 Throughput : 100
 Avg. Energy Level Of Nodes: 200 joules
 Delay Time : 12 m/s
 ************************************************
channel.cc:sendUp - Calc highestAntennaZ_ and distCST_
highestAntennaZ_ = 1.5,  distCST_ = 550.0
SORTING LISTS ...DONE!
arun@LM1 ~/Desktop/SelectiveForwardingAttack $ 
```

Fig 11 Experimental Results

This figure shows that the 32 packets send and received and also delivers Packet Delivery Ratio, Throughput, Average energy level of nodes, Delay time.

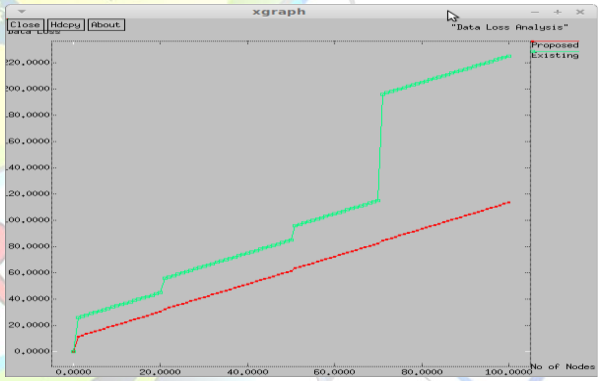


Fig 12 Data Loss Analysis

Fig 12 graph shows Data Loss versus No. of Nodes for existing and proposed system.

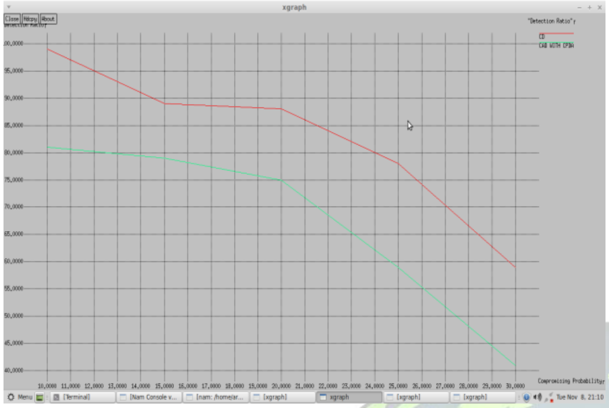


Fig 13 Detection Ratio

Fig 13 shows detection ratio versus comprising probability has CD and CAD with CPDA.

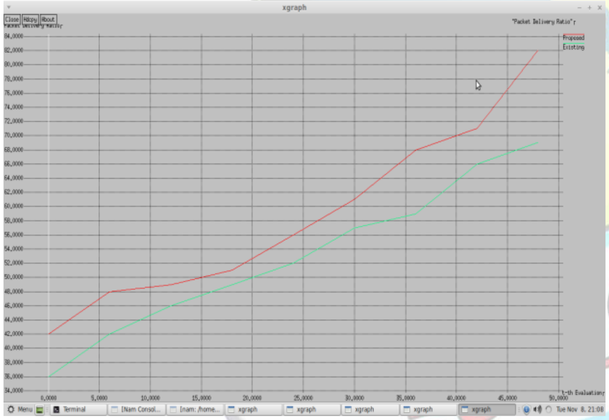


Fig 14 Packet Delivery Ratio

This graph figure shows PDR versus t-th Evaluation period for existing and proposed system.

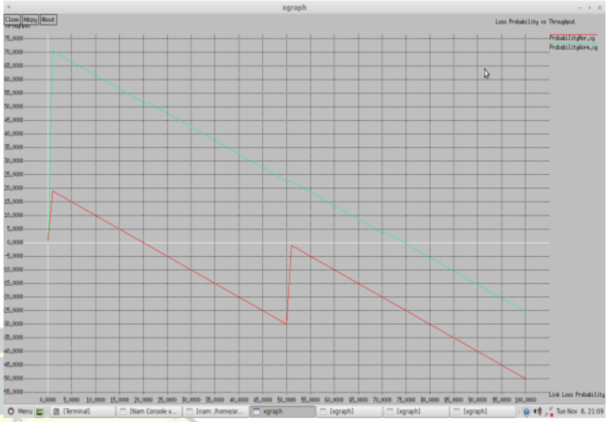


Fig 15 Loss Probability vs Throughput

Fig 15 shows Loss Probability versus Throughput for both normal and abnormal losses.

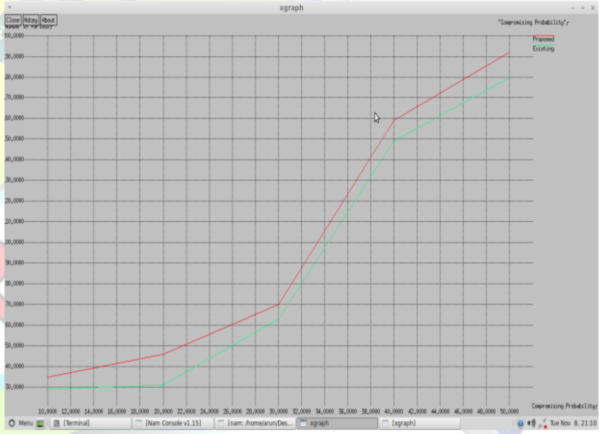


Fig 16 Comprising Probability

Fig 16 shows Comprising Probability versus No. of Periods for existing and proposed system.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Issue 11, November 2016

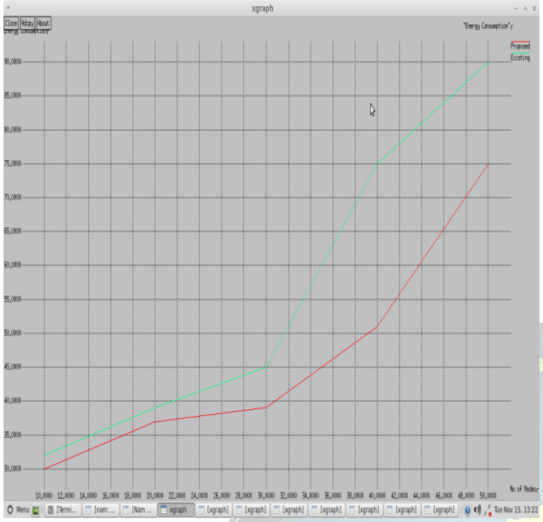


Fig 17 Energy Consumption

This graph shows No. of Nodes versus Energy Consumption for existing and proposed system.

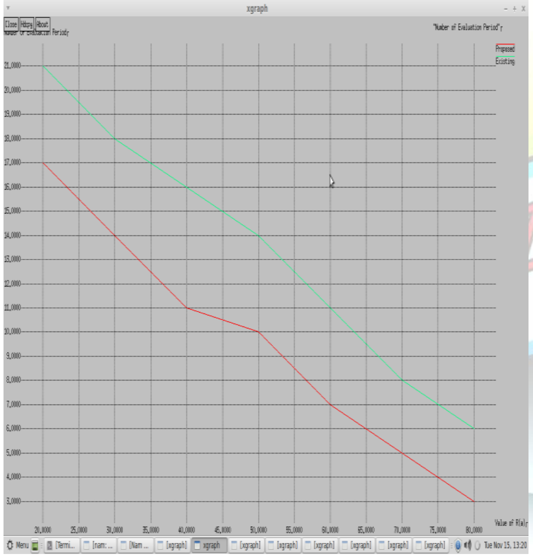


Fig 18 Number of Evaluation Period

Fig 18 graph shows Value of R(a) versus No. of Evaluation Period for both existing and proposed system.

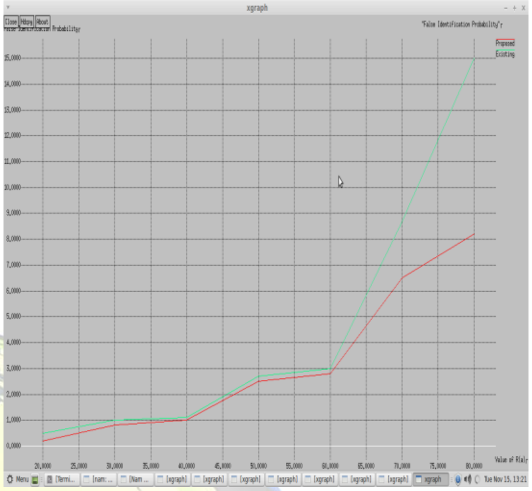


Fig 19 False Identification Probability

This above graph figure shows Value of R(a) versus false identification probability for both existing and proposed system.

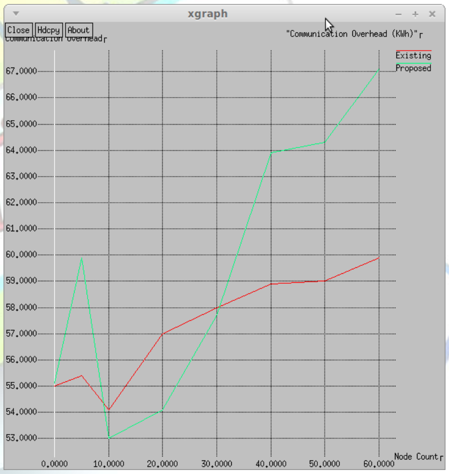


Fig 20 Communication Overhead

Fig 20 plotted graph between node count versus communication overhead for both existing and proposed system.

IV. CONCLUSION

In this project, propose a simple and efficient security scheme for detecting selective forwarding attacks. The attacks which affect it as in malicious node attack drop the packet and make it unavailable to destination. This type of attacks is important to meet the basic need of the n/w. So a Channel Based Identification (CBI) method is developed that can efficiently identify the selective forwarding attackers by filtering out the normal channel losses. The Channel Identification (CI) is integrated with Data Traffic Identification (DTI) to achieve channel-aware detection of selective forwarding misbehavior hidden in the normal loss events due to bad channel quality or MAC. These utilize the metric ETX to defend against selective forwarding attacks. Then proposed a Centralized Algorithm that assigns a central node to collect and analyze the forwarding behaviors of each node in the network. After that proposed a Distributed detection Algorithm against Wormhole in wireless Network coding systems, DAWN which is totally distributed for the nodes in the network eliminating the limitation of tightly synchronized clock. Both centralized and distributed algorithms utilized the digital signatures to ensure every report is undeniable and cannot be forged by any attackers. The simulations have shown that the proposed algorithms can detect the malicious nodes participating in selective forwarding attack with high successful rate and it is efficient in terms of computation and communication overhead. Currently this scheme can only discriminate abnormal packet loss from channel error packet loss at a high detection ratio. In future, plan to integrate the wormhole detection techniques with this scheme to find out the original causes of abnormal packet delay and thus reduce delay.

REFERENCES

[1]. Ju Ren, Yaoxue Zhang, Kuan Zhang, and Xuemin Shen, “Adaptive and Channel-Aware Detection of Selective Forwarding Attacks in Wireless Sensor Networks” IEEE Transactions on Wireless Communications, DOI 10.1109/TWC.2016.2526601

[2]. S. Ozdemir, “Functional reputation based reliable data aggregation and transmission for wireless sensor networks,” Computer Communication., vol. 31,no. 17, pp. 3941–3953, 2008.

[3]. X. Liang, X. Lin, and X. Shen, “Enabling trustworthy service evaluation in service-oriented mobile social networks,” IEEE Transaction Parallel Distribution Systems., vol. 25, no. 2, pp. 310–320, 2014.

[4]. Sophia Kaplantzis , Alistair Shilton , Nallasamy Mani , Y. Ahmet S¸ekercio glu ,” Detecting Selective Forwarding Attacks in Wireless Sensor Networks using Support Vector Machines”, intelligent sensors, sensor networks and information ,3rd international conference ,pg 335 – 340,ISSNIP 2007

[5]. Bo Yu and Bin Xiao. Detecting selective forwarding attacks in wireless sensor networks. In Parallel and Distributed Processing Symposium, 2006. IPDPS 2006. 20th International, page 8 pp., 2006.

[6]. Wang Xin-sheng, Zhan Yong-zhao, Xiong Shu-ming, and Wang Liangmin. Lightweight defense scheme against selective forwarding attacks in wireless sensor networks. pages 226 –232, oct. 2009

[7]. Anthony Wood, John A. Stankovic, “Denial of Service in Sensor Networks,” IEEE Computer, 35(10):54-62, October 2002.

[8]. S.Esakki Rajavel, C.Jenita Blesslin, “Energetic Spectrum Sensing For Cognitive Radio Enabled Remote State Estimation Over Wireless Channels”, International Journal of Advanced Research Trends in Engineering and Technology (IJARTET), Vol. 3, Special Issue 19, April 2016 (12 – 15).

[9]. Preeti Sharma1,Monika Saluja2 and Krishan Kumar Saluja,” A Review of Selective Forwarding Attacks inWireless Sensor Networks” International Journal Of Advanced Smart Sensor Network Systems (IJASSN), Vol 2, No.3, July 2012 DOI: 10.5121/ijassn.2012.2304 37

[10]. T. Ho, M. Medard, R. Koetter, D. R. Karger, M. Effros, J. Shi, and B. Leong, “A random linear network coding approach to multicast,” IEEE Transactions on Information Theory, vol. 52, no. 10, 2006.

[11]. S. Biswas and R. Morris, “Opportunistic routing in multihop wireless networks,” in ACM SIGCOMM, September 2004.

[12]. S. Chachulski, M. Jennings, S. Katti, and D. Katabi, “Trading structure for randomness in wireless opportunistic routing,” in SIGCOMM, August 2007.

[13]. D. Dong, Y. Liu, X. Li, and X. Liao, “Topological detection on selective forwarding attacks in wireless ad hoc and sensor networks,” IEEE Transactions on Networking, vol. 19, 2011.

[14]. J. Kim, D. Sterne, R. Hardy, R. K. Thomas, and L. Tong, “Timing based localization of in-band selective forwarding attacks tunnels in MANETs,” in ACM WiSec, 2010.

[15]. Muthukumaran. N and Ravi. R, 'The Performance Analysis of Fast Efficient Lossless Satellite Image Compression and Decompression for Wavelet Based Algorithm', Wireless Personal Communications, Volume. 81, No. 2, pp. 839-859, March 2015, Springer.

[16]. Muthukumaran. N and Manoj Kumar. B, 'Design of Low power high Speed CASCADED Double Tail Comparator', International Journal of Advanced Research in Biology Engineering Science and Technology, Vol. 2, No. 4, pp.18-22, June 2016.

[17]. Muthukumaran. N and Keziah. J, 'Design of K Band Transmitting Antenna for Harbor Surveillance Radar Application', International Journal on Applications in Electrical and Electronics Engineering, Vol. 2, No. 5, pp. 16-20, May 2016.

[18]. S. R. D. R. Maheshwari, J. Gao, “Detecting selective forwarding attacks in wireless networks using connectivity information,” in IEEE INFOCOMM, 2007.