Critical Event Monitoring For Packet-Block-Mechanism in Wireless Ad Hoc Networks

R.Latha [1], S.Sasikala [2]

[1]M.Phil Research Scholar, Department of Computer Science, Sree Saraswathi Thyagaraja College, Pollachi, TamilNadu, India - 642 107.

[2] Head, UG Department of Computer Science, Sree Saraswathi Thyagaraja College, Pollachi, TamilNadu, India - 642 107.

Abstract

Wireless ad hoc network is a decentralized type of wireless network. The network is ad hoc because it does not have any fixed infrastructure. One basic assumption of routing protocols in wireless ad hoc networks is every node is honest and cooperative. This nature introduces many security attacks. One of the attacks is the malicious packet dropping. Packet dropping attack is the most vulnerable attack. When the route is established from source to destination the malicious node drop the packets. The malicious node create wrong route between from source to destination which is leads to undesirable situation. In this paper we calculate high detection accuracy on lost packets. The accuracy is calculated by auto-correlation function (ACF) based on number of packets sent and lost. Sleep Scheduling for event monitoring is used to pass the message to other nodes in the network when critical event is detected.

Keywords: *Wireless attack, Packet dropping, malicious node, attack detection, Sleep Scheduling*

I. INTRODUCTION

Wireless ad hoc network is a de centralized type of wireless network. The network is ad hoc because it does not have any fixed infrastructure, such as routers in wired networks. Every node in the network is used to send the packets from source to destination. The nodes maintained dynamically based on available communications. Each node identifies the nodes that are available for communications, based on signal strength, which is mainly related to distance, but is also affected by obstructions or interference. Some nodes may be beyond range or weak signal. When the available nodes are identified the route is established and packet is forwarded to the destination.

A.MALICIOUS PACKET DROPPING

Malicious packet dropping is malicious node act as a legitimate node and drops the packets maliciously. It creates wrong route information from source to destination. Once the malicious node involved in routing it disturb the whole communication or drop the packet abruptly.

Once in the route, the malicious node can do anything including maliciously dropping packets. This Packet dropping at a malicious intermediate node can lead to suspension of communication or generation of wrong information between the source and destination which is an undesirable situation [7].

A malicious node drains the resource of the sender. Malicious node does not sending acknowledgement to the sender after receiving the packet. The sender will assume that the packet is not forwarded correctly. So sender sends the packets many times. When malicious node send acknowledgement with data packet the sender assume that the

Packet forwarded correctly. Then the route is routed through malicious node and packets get dropped.

II. PROBLEM DEFINITION

In wireless ad hoc networks, nodes communicate with each other using multi hop wireless links. Data to out of range nodes can be routed through intermediate nodes. That is nodes in wireless ad hoc networks can act as both hosts and routers [7]. The nodes dynamically establish paths among one another. But, the lack of centralized management of these networks makes them vulnerable to a number of security attacks. One of the attacks is packet drop attack, where a compromised node drops packets maliciously.

Nodes in wireless ad hoc networks have limited energy resource. Intermediate nodes in these networks may behave selfishly and fail to forward the received packets in order to conserve their limited resources battery power. These packets in turn get dropped [7].

The Proposed algorithm used to find the detection accuracy of lost packets. Calculating the correlation between numbers of packets sent and lost. Using this correlation the position of lost packets identified correctly. We can easily identify the packet loss whether it caused by malicious attack or other conditions. This method gives high detection accuracy and truthfulness of packet loss.

The Level-by-level offset schedule Algorithm is used to achieve low broadcasting delay in a large scale wireless Networks. After detection of malicious node center node send the alarm message to the cluster heads, then the alarm passed from cluster head to other nodes in the network. In sleep scheduling the nodes are maintained in sleep mode until data arrives for energy minimization.

III. PROPOSED METHOD

- Detecting the correlations between the lost packets is based on number of packets sent and lost. It denoted by 0 (loss) and 1 (no loss). That is Number of packets successfully received, and number of packets lost
- Each node reports its status about received packets/ lost packets. Some attacker nodes gives false report for avoid being detected by detection algorithm. So truthfulness of the nodes is important for calculation.
- To resolve this problem, auto correlation function is used to identify the actual status of the nodes and packet loss. Using this method we can easily identify packet loss whether it is caused by malicious attack or other conditions
- The Level-by-level offset schedule Algorithm is used to achieve low broadcasting delay in a large scale wireless Networks. When critical event is detected center node send the alarm message to the cluster heads, then the alarm passed from cluster head to other nodes in the network. In sleep scheduling the nodes are maintained in sleep mode until data arrives for minimizing the energy consumption of nodes.

A. ALGORITHM STEPS FOR THE PROPOSED SYSTEM

Step 1: Initializing the packet rate based on packet size

Step 2: Initializing node availability space for Packet weight

Step 3: Calculating detection accuracy using ACF and HLA

Step 4: Initializing and calculating link errors rate based on route

Step 5: Establish the routing.

Step 6: Verifying the packet rate in each and every nodes

Step 7: Calculating for detection accuracy in each route.

Step 8: Calculating receiving packet rate based on nodes.

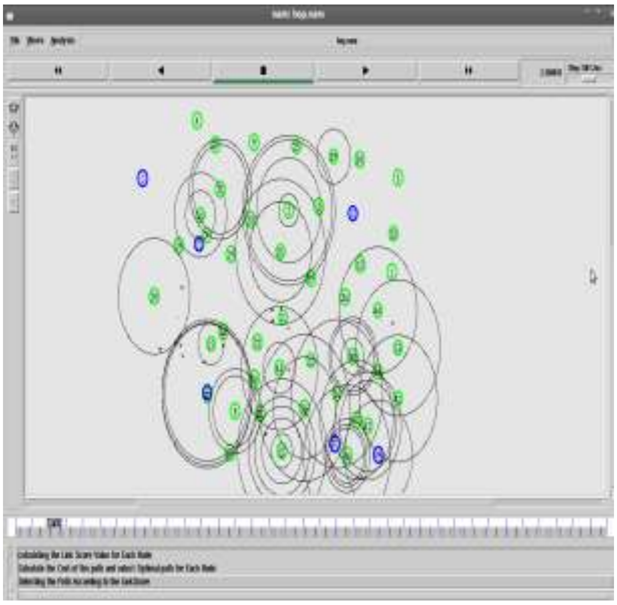
Step 9: Updating packet rate based on nodes.

Step 10: Calculating route node accuracy.

B.PROPOSED SYSTEM IMPLEMENTATION:

Calculating link score value:

Calculating link score value for each node in the network and also calculating cost of the path to find the optimal path from source to destination.

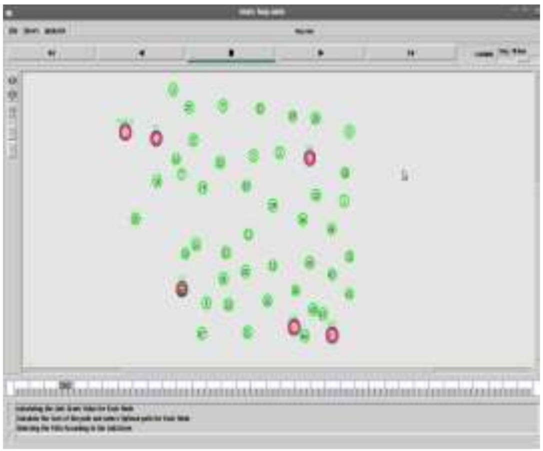


Calculating Correlation between nodes:

Correlation is calculated by number of packets sent and number of packets lost. Individual node reports it status

Cluster heads and Center node:

Center nodes pass the message to cluster heads. Cluster head monitor the group of nodes and pass messages to them.

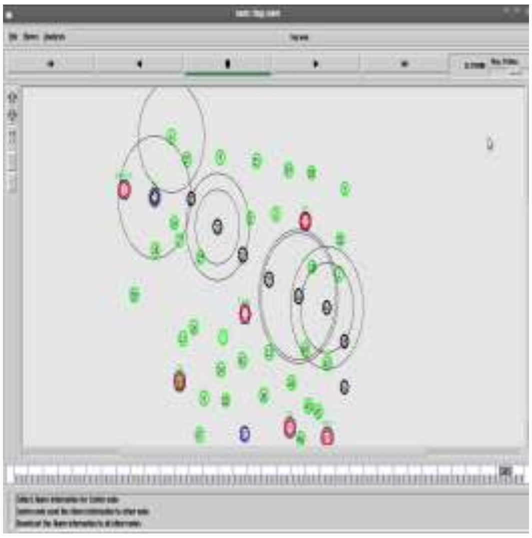


Malicious node identification:

Malicious node is identified by algorithm which has high packet loss rate and high energy consumption

Alarm message:

Alarm message passed from center node to cluster head then it pass messages to all other nodes in the network. The malicious node will be blocked. Data packet is sent from source to destination securely.



IV. RESULTS AND DISCUSSION

The performance evaluation of the proposed system is analyzed to prove the efficiency of the scheme. The entire model is simulated through NS2 Network Simulator.

Network simulator

Ns is a public domain simulator boasting a rich set of Internet Protocols, including terrestrial, wireless and satellite networks. Ns is the most popular choice of simulator used in research papers appearing in select conferences like Sigcomm. Ns is constantly maintained and updated by its large user base and a small group of developers at ISI.

Ns is a discrete event simulator targeted at networking research. It provides substantial support for simulation of TCP, routing, and multicast protocols over wired and wireless (local and satellite) networks. It includes an optional network animator.

TABLE:
SIMULATION PARAMETERS

Description	Value
Simulator	NS2
Protocol	AODV
Simulation Area	1900mX 1900m
Simulation duration	35 Ms
Transmission range	256 m
Pause time	0.048
Packet Size	256 bytes
Packet rate	1024 bytes

The following metrics Energy, Packet- drop, Error Detection, Miss-Detection and False-Alarm are to evaluate the performance of the proposed mechanism.

ENERGY CONSUMPTION

Energy consumption is a significant issue in ad hoc networks since mobile nodes are battery powered. In order to prolong the lifetime of ad hoc networks, it is the most critical issue to minimize the energy consumption of nodes.

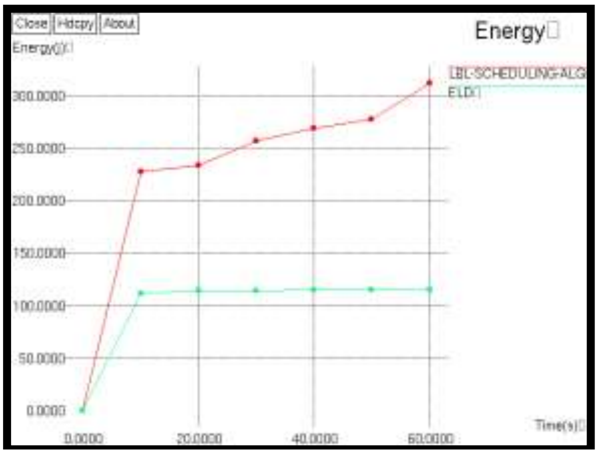


Figure 4.1 Energy Efficiency by nodes for various times

The proposed system has high energy efficiency than existing systems. The result is shown in Figure 4.1.

PACKET – DROP

Packet drop is packets may dropped due to link errors or malicious node and other reasons while transmission from source to destination

The proposed system minimizes the packet drop rate than existing methods. The result is shown in Figure 4.2

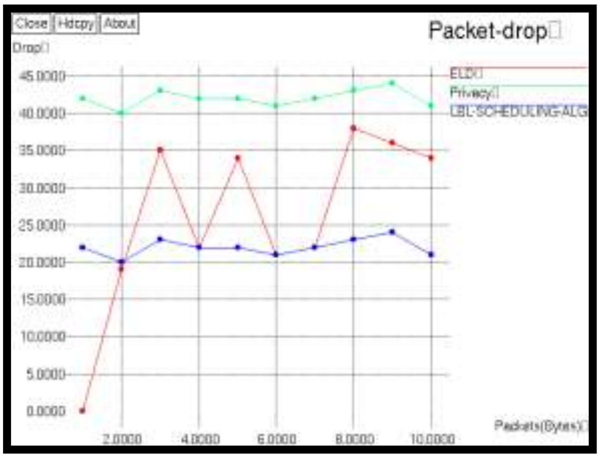


Figure 4.2 Packet drop rate vs. Packets sent

ERROR DETECTION

Error detection is the detection of errors caused by noise or other impairments during transmission from the transmitter to the receiver. Error detection is a technique that enables reliable delivery of digital data over unreliable communication channels.

In this proposed method detection of error is reduced than existing methods. The result is shown in Figure 4.3

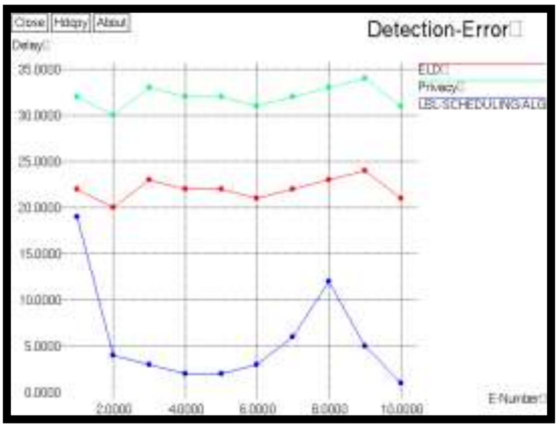


Figure 4.3 Error Detection during Packet transmission

MISS DETECTION

Miss Detection is the normal nodes identified as malicious node.

In this proposed method miss detection probability is reduced with respect to the number of packet drop rate. This result is shown in Figure 4.4

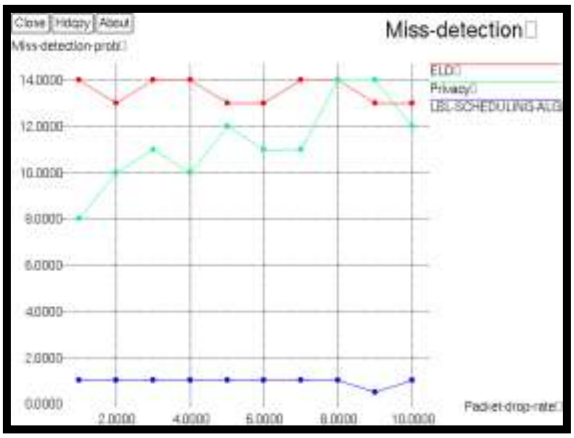


Figure 4.4 Miss- Detection Probability vs. Packet drop rate

FALSEALARM

False Alarm is alarm packet is raised when the critical event is detected. An alarm will be raised based on the malicious behaviour of nodes. An alarm packet is broadcasted to the entire network when critical event is detected.

In this proposed method an alarm packet is raised highly than existing method, when critical event is detected. The result is shown in Figure 4.5

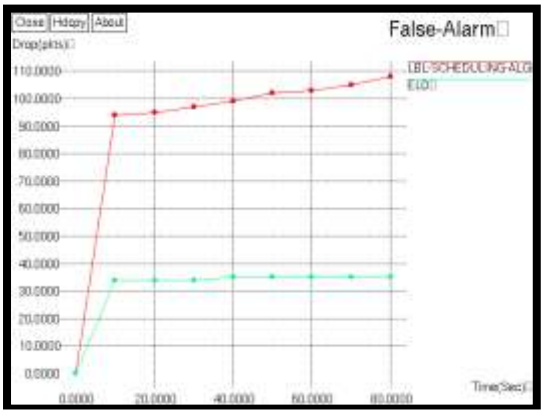


Figure 4.5 Alarm raise when Critical event detected

V.CONCLUSION

Packet dropping attack is serious problem in wireless ad hoc network. The proposed method finds the packet loss and its position effectively. Using this method the packet dropping is identified easily. Sleep scheduling for event monitoring is used for energy minimization.

FUTURE ENHANCEMENT

This paper provides a comprehensive study and evaluation from different perspectives, still some issues and several research directions that can be pursued. The proposed mechanism under various particular protocols will be considered for future studies. Detection of misbehaving source and destination increase the probability of success rate of packets will be pursued in future work.

REFERENCES

[1.] Bora Karaoglu, Wendi Heinemann, ”Cooperative Load Balancing and Dynamic Channel Allocation for Cluster-Based Mobile Ad HocNetworks”.IEEE transactions on mobile computing, vol. 14, no. 5, may 2015.

[2] Jian-Ming Chang, Po-Chun Tsou, Isaac Woungang, Han-Chieh Chao,and Chin-Feng Lai, “Defending Against Collaborative Attacks by Malicious Nodes in manets: A Cooperative Bait Detection Approach” IEEE systems journal, vol. 9, no. 1, march 2015

[3] Xin Ming Zhang, Yue Zhang, Fan Yan, and Athanasios V. Vasilakos, “Interference-Based Topology Control Algorithm For Delay-Constrained Mobile Ad Hoc Networks”, IEEE transactions on mobile computing, vol. 14, no. 4, April 2015

[4] Karan Mitra, Arkady Zaslavsky, and Christer Åhlund,” Context-Aware QoE Modelling, Measurement, And Prediction in Mobile Computing Systems”, IEEE transactions on mobile computing, vol. 14, no. 5, may 2015

[5]Bodhy Krishna S "An Overview of the Existing Routing Protocols and Trust Based Algorithms in Mobile Ad-hoc Networks ". International Journal of Computer Trends and Technology (IJCTT) V20(1):19-27, Feb 2015. ISSN:2231-2803.

[6] Vikram R. Desai, "Techniques for detection of malicious packet drops in networks", masters theses 1896 - february 2014

[7] Kennedy Edemacu, Martin Euku and Richard Ssekibuule ,” Packet drop attack detection techniques in wireless ad hoc networks: a review”, International Journal of Network Security & Its Applications (IJNSA), Vol.6, No.5, September 2014

[8] Ze Li, Haiying Shen, “A QoS-Oriented Distributed Routing Protocol for Hybrid Wireless Networks”. IEEE transactions on mobile computing, vol. 13, no. 3, march 2014.

[9] Er. Priyanka goel , Dr. Pankaj kumar verma, “Detection and isolation of selective Packet drop attack in manet Using diffie - hellman algorithm”.
International Journal of Latest Research in Science and Technology Volume 3, Issue 3: Page No. 137-139, May-June 2014

[10] Kshitij Bhargava, Dinesh Goyal, “Packet dropping attacks in Manet: a survey”. Journal of Advanced Computing and Communication Technologies, Volume No.2 Issue No. 3, June 2014

[11] You-Chiun Wang,” A Two-Phase Dispatch Heuristic to Schedule The Movement of Multi-Attribute Mobile Sensors in a Hybrid Wireless Sensor Network”, IEEE transactions on mobile computing, vol. 13, no. 4, April 2014.

[12] Glory Rashmi. A, Mr.C.Murugesh ,” Detection of Clone Nodes in Mobile Sensor Networks using Distributed and Localized Algorithms” International Journal of Inventions in Computer Science and Engineering Volume 1 Issue 2 2014

[13] Raju M, Selvan M,” An Approach in Detection of Replication Node in Wireless Sensor Networks: A Survey”, International Journal of Computer Science and Information Technologies, Vol. 5 (1) ,2014, 192-196

[14]S.Ganesan, B.Loganathan "A Survey of Ad-Hoc Network: A Survey" International Journal of Computer Trends and Technology (IJCTT),*V4(8):2652-2655* August Issue 2013 .ISSN 2231-2803

[15] S.Vijayalakshmi, R.Kurinjimalar, S.Prakash, “Detection of Packet Dropping and Modification in Wireless Sensor Network”, International Journal of Computer Science & Engineering Technology (IJCSET), ISSN: 2229-3345 Vol. 4 No. 04 April 2013.

[16] Shalini Sharma, Proff. Mr. Hitesh Gupta, Proff. Mr. Pankaj Kawadkar, “Reducing Packet Loss in MANET”, Network and Complex Systems, Vol.3, No.6, 2013.

[17] Khajonpong Akkarajitsakul, Ekram Hossain, Dusit Niyato, “Cooperative Packet Delivery in Hybrid Wireless Mobile Networks: A Coalitional Game Approach”, IEEE transactions on mobile computing, vol. 12, no. 5, may 2013.