# AN ENERGY EFFICIENT TRUTHFUL DETECTION PACKET LOSS BASED ON ENERGETIC ROUTING PROTOCOLS

AISHWARYA . S , MOORTHY . C , DEVIKA . B , DEEPA . R , GOBIKA . K

***Abstract*—** Wireless and ad hoc networks have gained much importance due to its simplicity and low cost of deployment. The decentralized management of this network makes it susceptible to various attacks. Packet dropping is one of the major security issue. Mobile ad hoc networks is a kind of ad hoc wireless networks in nodes are mobile.This paper presents packet dropping and packet dropping attack detection technique in Energy based Routing Protocol.This paper concludes with the necessity of motivating a malicious node in case of malicious packet dropping in wireless ad hoc networks.

***Keywords*—** Packet Dropping , Network .

## I. INTRODUCTION

Wireless ad hoc network is one of the category of wireless networks which operates without the support of any fixed infrastructure.Due to itself organizing behavior ad hoc networks are mainly used in military applications,emergency operation and disaster recoveries. Packet loss is a serious issue in wireless networks. There are several classifications for packet dropping and packet dropping detection techniques[1].The major classification for packet dropping includes legitimate packet dropping,stealthy packet dropping and malicious packet dropping.In case of mobile node,mobility is also a reason for packet loss.

Aishwarya . S , Department of Electronics and Communication Engineering , VSB Engineering College , Karur .
( Email ID : aishw955@gmail.com )
Moorthy . c , Department of Electronics and Communication Engineering , VSB Engineering College , Karur .
( Email ID : moorthy.ind@gmail.com )
Devika . B , Department of Electronics and Communication Engineering , VSB Engineering College , Karur .
( Email ID : devika2731@gmail.com )
Deepa . R , Department of Electronics and Communication Engineering , VSB Engineering College , Karur .
( Email ID : deepakarthick12@gmail.com )
Gobika . k , Department of Electronics and Communication Engineering , VSB Engineering College , Karur .
( Email ID : gobikaraj1997@gmail.com )

Energy efficiency is an essential requirement for WSN to maximize the life time of the network.By using cluster tree also we can increase the energy of the network.

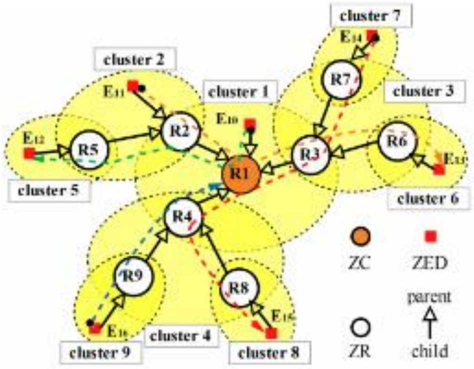


Figure 1:Cluster tree WSN and four time-constrained data flows

In the existing method,they use scheduling algorithm to avoid collision and by using it we can transmit the packet from end to end deadline of each flow given in time units.

### 1) Packet Dropping:

### A. Legitimate Packet Dropping

Legitimate packet dropping in which no compromised nodes are there may occur due to network congestion,channel condition and resource constraints.

- Network Congestion:

Congestion is one of the crucial factor which leads to packet loss.scalability is possible in ad hoc wireless networks due to the movement of nodes which is also a cause for congestion.

- Channel Condition:

Interference,free path loss,presence of noise on the channel arecertain channel condition.These factors lead to packet dropping or bit error in the signal which is transmitted.

- Resource Constraint:

Energy is one of the resource constraints that have to be considered with great importance.The nodes having limited energy saves their energy by not forwarding packets. Thisselfish behavior of the nodes leads to packet drop.

### B. Stealthy Packet Dropping

Stealthy packet dropping launch attacks that are harmful as brute force attacks.It minimizes the cost and the visibility of the attack[2].Stealthy packet dropping attack types are

Power Control
Misrouting
Colluding Collision
Identity Delegation

### C. Malicious Packet Dropping

Packet dropping due to malicious nodes which takes part in the route during data transmission is termed as malicious packet dropping. An intermediate node which is malicious can even suspended the communication or generate wrong information between the source and the destination.

## II. Related work

To develop an accurate algorithm for detecting selective packet drops made by insider attacker.High detection accuracy is achieved by exploiting the correlations between the positing of lost packet,as calculated from the autocorrelation function (ACF)of the packet loss bitmap a bitmap describing the lost /received status of each packet ina sequence of consecutive packet transmission. By detecting the correlation between the lost packets, one can decide whether the packet loss is purely due to regular link errors, or is a combined effect of link error and malicious drop.The main challenge in our mechanism lies in how to guarantee that the packet loss did not reported by individual nodes along a route are truthful. Such truthfulness is essential for correct calculation of the correlation between lost packets, this can be achieved by some auditing.Considering that a typical wireless device is resource constrained,we also require that a user should able to delicate the burden of auditing and detection to some public server to save its own resources. Public auditing problem is constructed based on the homomorphic linear authenticator(HLA)cryptographic primitive, which is basically a signature scheme widely used in cloud computing and storage server systems to provide a proof of storage from the server to entrusting claims .

## III. Block Diagram

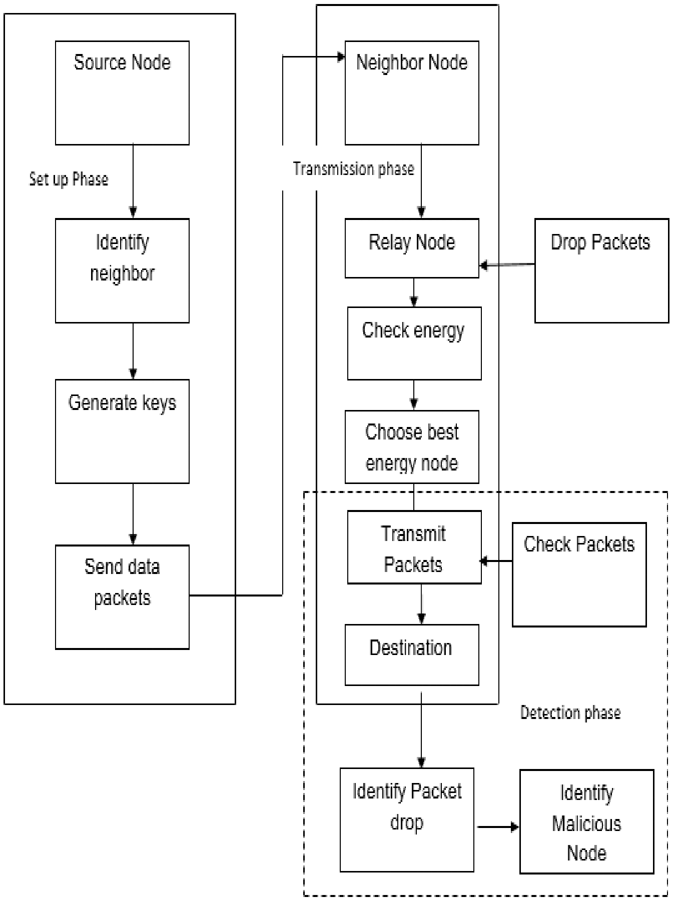


Figure 2: System Architecture

**Block Diagram Explanation**

There are three types of phase are available energy based routing protocol. They are, setup phase, transmission phase, detection phase.

**Setup phase**The phase takes place right after route Psd is established, but before any data packets are transmitted over the route .In this phase,S decides on a symmetric key cryptosystem ( encrypt key, decrypt key) and K symmetric keys key1,…,keyK where encrypt key and decrypt key are the keyed encryption and decryption functions,respectively. S securely distributes decrypt key and symmetric key Kj to node mj and sends the cipher text to nj. Nj decrypt the cipher text using its private key to obtain key j.

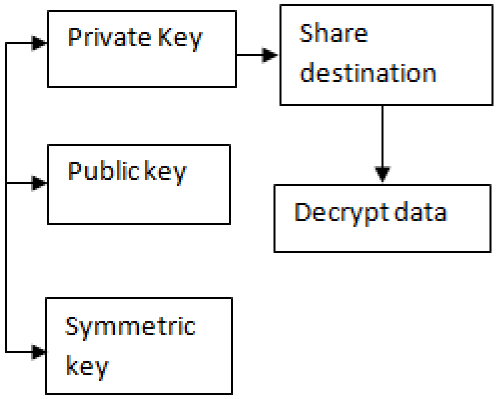


Figure 3

**Transmission phase** This part is fully based on energybassed routing protocol.Energy based routing is performed by using BFS (Breadth First Search) algorithm. The BFS begins at aroot node and inspects all the neighboring nodes. Then for each of those neighbor nodes in turn,it inspects their neighbor nodes which were unvisited.This helps to generate a feasible path rooted towards destination. Thus the energy consumption for packet transmission can be decreased.

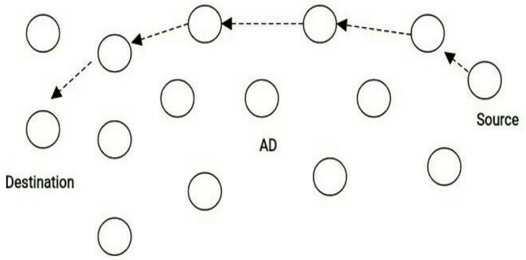


Figure 4: Network model

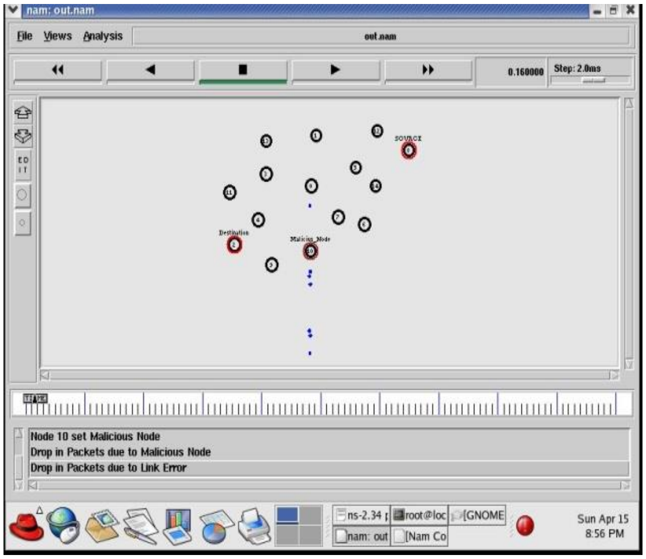
**Detection phase**There are two main process are involved in detection phase.Those are as follows.

- Packet drop identification

Here the mechanism is based on detecting the correlations between the lost packets over each hop as a random process alternating between 0(loss)and 1(no loss) . Specifically consider that a sequence of M packets that are transmitted consecutively over a wireless channel . Under different packet dropping conditions, i.e., link error vs malicious dropping the instantiations of the packet loss random process should present distinct dropping patterns. When there is link error, the packet loss may be minimum. When there is a malicious node dropping packet, the loss will be high.

- **Malicious node identification**

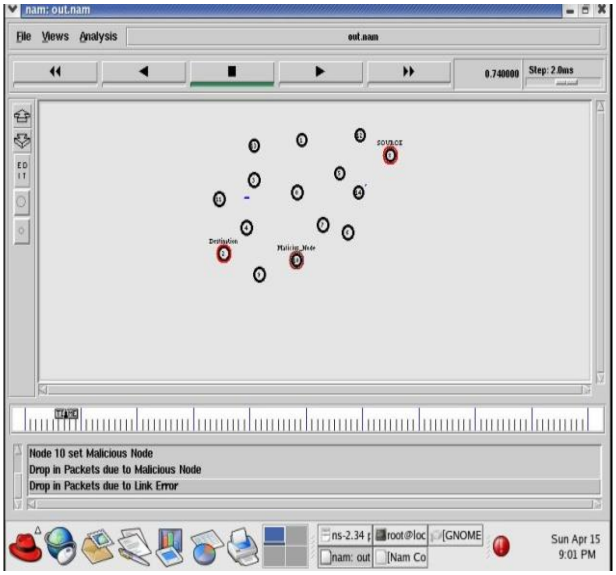
There is an independent auditor Ad in the network. Ad is independent in the sense that is not associated with any node in Psd and does but have any knowledge of the secrets held by various nodes. The auditor is responsible for detecting malicious nodes on demand. Specifically, that is assumed S receives feedback from D when D suspects that is the route is under attack. Once being notified of possible attack,S Submits an attack detection request(ADR) to Ad.To facilitate its investigation,Ad needs to collect certain information from the nodes on route Psd. Each such node must reply to Ad ‘s inquiry, otherwise the node will be consider as misbehaving. Normal node reply with truthful information, but malicious node may cheat.At the same time , for the privacy reasons ,it is require that Ad cannot determined he content of the normal packets delivered over Psd from the information collected during the auditing .



```
Node 10 set Malicious Node
Drop in Packets due to Malicious Node
Drop in Packets due to Link Error
```

Figure 5: Malicious node Identification

Most of the related works assumes that malicious dropping is the only source of packet loss



```
Node 10 set Malicious Node
Drop in Packets due to Malicious Node
Drop in Packets due to Link Error
```

Figure 6: packet through Energy based routing path

## IV. SIMULATION STUDY

The simulation model is implemented on simultator and configured based on the AODV routing Algorithm. Figure 5 Malicious node identification in which the node then is identified as malicious node by independent auditor and the drop is due to intentional or unintentional is also identified.Intentional it means malicious node and unintentional means link error. Fig 3.1 the packet is intentional ( malicious node)

Figure 6 In which by using AODV routing algorithm a successful packet transmission from source to destination is obtained without packet dropping.

### Graphical representation:

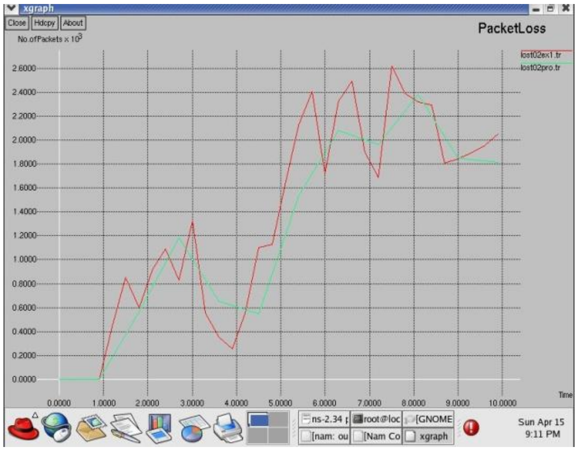


Figure 7 : Packet drop rate

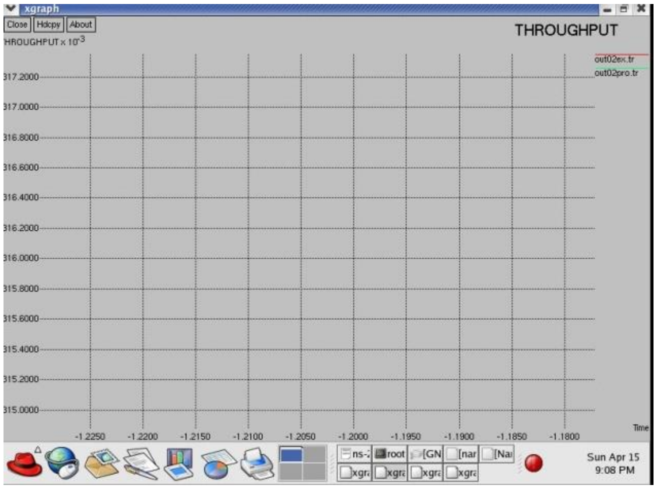


Figure 8: Transmission throughput

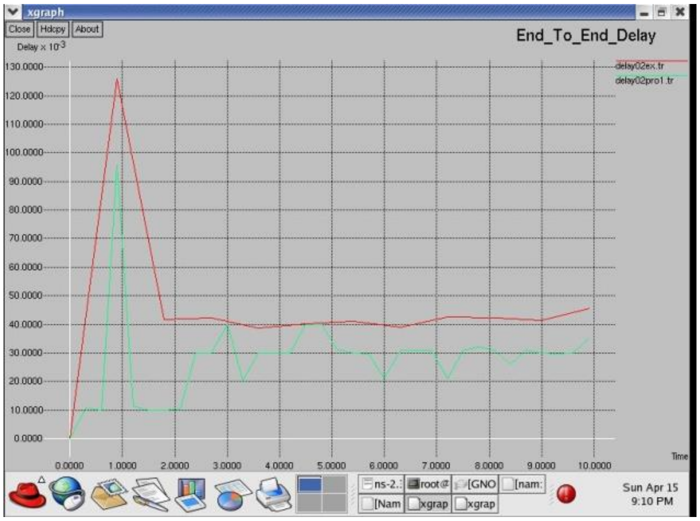


Figure 9: End to End delay

## V. CONCLUSION

Packet dropping is the major factor for loss of packet in wireless adhoc networks.Malicious packet dropping due to the intentional attack of malicious nodes is one of the important packet dropping attacks.packet dropping attack detection techniques have several limitation.Mobility features must be considered during detection of malicious nodes.Isolating malicious nodes after detection will affect the performance of the network.Thus there is a need to motivate the malicious nodes detected in order to make them inactive again in wireless adhoc networks.

## REFERENCES

[1] An Energy Efficient Schedule for IEEE 802.15.4/ ZigBee Cluster Tree WSN with Multiple Collision Domains and

Period Crossing Constraint Aasem Ahmad and Zdenˇek Hanz´alek2017.

[2] Tao Shu and Marwan Krunz, ”Privacy-Preserving and Truthful Detection of Packet Dropping Attacks in Wireless Ad Hoc Networks”, IEEE Transactions on Mobile Computing, Vol.14, No.4, April 2015.

[3] W. Liu, D. Zhao, and G. Zhu, “End-to-end delay and packet drop rate performance for a wireless sensor network with a cluster-tree topology,” Wireless Communications and Mobile Computing, vol. 14, no. 7, 2014.

[4] SoufieneDjahel, Farid Nait-abdesselam, and Zonghua Zhang, ”Mitigating Packet Dropping Problem in Mobile Ad Hoc Networks: Proposals and Challenges”, IEEE Communications Surveys and Tutorials, Vol 13, N0.4, Fourth Quarter 2011.

[5] Issa Khalil and Saurabh Bagchi, ”Stealthy Attacks in Wireless Ad Hoc Networks: Detection and Countermeasure”, IEEE Transactions on Mobile Computing, Vol 10, No.8, August 2011.

[6] K. Balakrishnan, J. Deng, and P. K. Varshney. TWOACK: preventing selfishness in mobile ad hoc networks. In Proceedings of the IEEE WCNC Conference, 2005.