Robust Intrusion Detection Mechanism for Mobile Adhoc Networks

Ms. Rasagna Chinthireddy[1] & Dr. S Arvind[2]

[1]Dept. of CSE, CMRIT, JNTU, Kandlakoya, Hyderabad

[2]Dept. of CSE, CMRIT, JNTU, Kandlakoya, Hyderabad

***Abstract*— Due to their natural mobility and scalability, Mobile Adhoc NETworks (MANETs) are always preferred since the day of their invention. But the open medium nature of MANETs makes them more vulnerable to attacks and hence results in the degradation of performance. This paper proposes an ideal Intrusion Detection System called RIDM- Robust Intrusion Detection Mechanism that works with the backbone as EAACK, thus an approach that increases the performance of EAACK through Energy based Geographic Routing Protocol and also an attempt to reduce the Routing Overhead caused by acknowledgement packets in EAACK through Batch Processing.**

***Keywords*—IDS, EAACK, Energy based Geographic Routing Protocol, Batch Processing.**

I. INTRODUCTION

A Mobile Ad Hoc Network (MANET) is an infrastructure less network which is formed by a collection of mobile nodes that communicate with each other via wireless links directly or with the help of intermediate nodes. Nodes in a MANET are equipped with both a wireless transmitter and a receiver that communicate with each other via bidirectional wireless links either directly or indirectly. Routing protocols such as DSR, AODV, ZRP etc., can be used to determine the route from a node to another node. Due to its nature of open medium, the MANETs may have severe threats posed by attackers or malicious node. Nodes in the network move rapidly and hence there is no fixed network topology for MANETs.

There are two types of MANETs:

- Closed MANETs
- Open MANETs [1]

1)*Closed MANETs*— In close MANETs all the mobile nodes work collaboratively to accomplish a common goal. Eg: Military operations.

2)*Open MANETs*— In open MANETs all the nodes in the network have their own goals, yet they share their resources to accomplish some global activity.

Some resources in the network will be consumed very quickly, such as battery power of mobile nodes. The nodes in the network may sometimes act as misbehaving nodes or sometimes behaves selfishly. For example, a node may attempt to benefit the resources from other nodes in the network but may refuse to share its own resources. Such nodes are called Selfish nodes or Misbehaving nodes. Another example is a selfish node may refuse to forward data packets to other nodes in the network so as to conserve its energy.

II. INTRUSION DETECTION SYSTEMS

Intrusion Detection System is a security management system that monitors network traffic to detect suspicious activities attempted by nodes in the network. Various schemes have been proposed to prevent selfishness in MANETs. Intrusion Detection Systems are broadly classified into three categories shown below:

- Credit-based schemes.
- Reputation-based schemes.
- End-to-End Acknowledgement Scheme

A.Credit-Based Schemes

A credit is given to every node so that they can provide services to every other node in the network. To achieve this, virtual currency system can be set up. Every node in the network is paid for providing services to other nodes in the network. Whenever a node provides service it gets paid for it, and in turn pays the credit when it requests other nodes to help it in forwarding the packets [2], [4], [5], [6]. **Buttyan** [2] and **Hubaux** [2] proposed a concept of nuggets or beans to be paid by each node to the other nodes for helping them in packet forwarding.

As a result two models were proposed:

a) The Packet Purse Model [2]

b) The Packet Trade Model [2]

B.Reputation- Based Schemes

1) Watchdog & Path rater Scheme

The Watchdog [7], [8], [9], [10], [11] scheme is the IDS that detects misbehaving nodes in the network formed by mobile nodes. Watchdog is installed in all the nodes of the MANET. Whenever a node forwards a packet to the next node in the path to reach the destination, the watchdog installed in the node ensures that the next node in the path forwards the packet by overhearing the transmission promiscuously. Any node that does not forward the packet it receives will have its counter value incremented. If the counter value of any node exceeds threshold set prior, such node is tagged malicious and is avoided in the future transmission.

Pathrater [12] works in collaboration with the routing protocols in deciding which path to destination must be chosen to transmit the packets. Every node uses the information provided by watchdogs to rate neighbor nodes. Each node in the network maintains the reliability rating for every other node in the network. Pathrater calculates the rating of each path from source to destination by taking the average of ratings all the nodes involved in the path.

The weaknesses of Watchdog scheme are namely, false misbehavior, limited transmission power, and receiver collision.

C. End – End Acknowledgement Schemes

1) 2ACK SCHEME

The 2ACK scheme proposed by **Liu** *et al.[14]* is a network-layer technique to detect misbehaving links. The 2ACK scheme detects misbehavior through using acknowledgment packet namely 2ACK. This packet is sent by a node to two nodes down the line along the route.

Fig. 1 illustrates the operation of the 2ACK scheme. From the figure it can be seen that *N*1, *N*2, and *N*3 are three consecutive nodes along the transmission path.

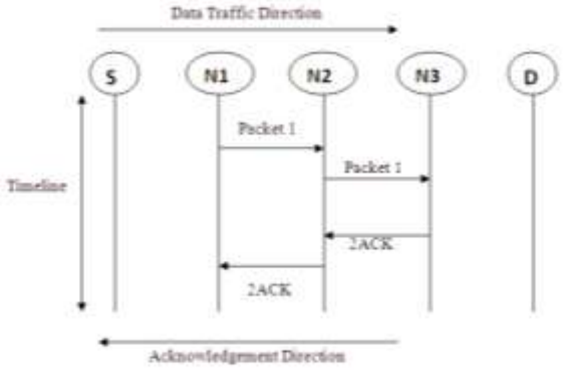


Fig 1: 2ACK scheme

2ACK scheme ensures that each node sends an acknowledgement packet two hops down the line along the route in opposite direction i.e. Node N3 on successful reception of data packet must send the acknowledgement 2ACK to N1 via N2. This acknowledgment 2ACK contains ID of the corresponding data packet received by N3.

Each node in the transmission path maintains the list of IDs of packets that are sent from it for a predefined time say T seconds. If the 2ACK is received within T seconds, then the ID of that packet will be deleted from list at the node receiving 2ACK. Otherwise the ID is deleted from the list after T seconds and failure count will be incremented.

III. PROPOSED SYSTEM

The proposed system is an Intrusion Detection System named as RIDM- Robust Intrusion Detection Mechanism that mainly works with the backbone of EAACK an acknowledgement based scheme proposed by Elhadi M. Shakshuki et al. [13]. This paper aims at improving the performance of existing IDS EAACK.

A. Energy based Geographic Routing Protocol

The Routing Protocols are mainly classified into two categories as Topology Based and Position Based. Mobile Adhoc Networks change their topology frequently & without prior notice, routing becomes a challenging task. Position based routing protocols also called as Geographic Routing Protocol [3] has many advantages over topology based protocols. These protocols require information such as physical location of nodes in the network. Each node determines its location using GPS or any other location service. It mainly focuses on two important aspects: location service to determine next node in the path and s forwarding technique that is used to forward the packets in the network.

The forwarding technique used in this paper is greedy forwarding. The routing decision is thus based on position of destination as well as position of neighbor of the node that forwarded the packet.

Therefore this routing technique does not require routing tables to be maintained.

1) Euclid's distance formula

Several paths are found from source to destination [3]. Hence it becomes necessary to determine which is the best path or the shortest path from source to destination. In this paper the Euclid's distance formula [3] is used to determine the distance between two nodes.

$$\mathbf{d}= \sqrt{(\Delta \boldsymbol{x})^2 + (\Delta \boldsymbol{y})^2}$$

$$= \sqrt{(\boldsymbol{x2} - \boldsymbol{x1})^2 + (\boldsymbol{y2} - \boldsymbol{y1})^2}$$

where, d is the distance between two nodes and x1, y1 and x2, y2 are the coordinate position of two nodes.

Sometimes it may so happen in MANETs that a node may get compromised and become a malicious node without forwarding the packets it received, or it may intentionally restrict its transmission range so as to safe guard its battery from getting drained. A node which is always selected as the one in the source destination path may get its battery drained and hence will not be able to transfer data any more, in which case such mode may be treated as malicious though it is an innocent node.

When two nodes are at the same distance to the destination, in this paper the energy (in Joules) parameter of the node is considered to avoid packet loss due to battery draining problem. The node that has more energy is considered as the one in the path.

B. Modules of RIDM

Compared to the contemporary approaches of for intrusion detection in MANETs, the EAACK [13] demonstrates a higher rate of malicious node detection but does not greatly improve the performance of network.

The drawbacks found in EAACK are: huge number of acknowledgement packets generated for data packet being sent and also no encryption done to the data packet on the sender side.

Hence in this paper, RIDM, DES algorithm is used to encrypt data on the sender side.

All the end-end acknowledgement schemes deal with acknowledgement packets which need to be authenticated.

As in EAACK [13] the proposed system RIDM also consists three major parts:

- End – End Acknowledgement Scheme (ACK)
- Secured Acknowledgement Scheme (S- ACK)
- Misbehavior Report Authentication (MRA)

1)ACK Scheme

ACK is an end-to-end acknowledgment scheme. ACK aims at reducing the network overhead caused due to acknowledgement packets.

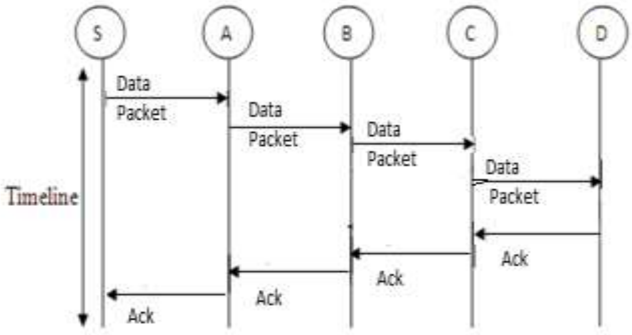


Fig 2: ACK scheme

Fig. 2, illustrates the operational details of ACK mode, node S forwards a data packet to destination node D. All the nodes in the transmission path collaboratively work to forward the data packets to destination node D. On successful reception of data packet in a batch, the destination node D responds back to source node by sending it an acknowledgement packet down the line. If the source node receives the acknowledgement packet within the time set then it is considered to be a successful data transfer. Otherwise the source node switches itself to the S-ACK mode by forwarding an SACK packet to detect the misbehaving nodes in the transmission path.

2)S- ACK mode

The S-ACK scheme as proposed by **Liu** *et al.* [14] is an improved version of the TWOACK scheme. The goal of SACK scheme is to let every three consecutive nodes to collectively work as a group in identifying the misbehaving nodes. The third node in the triplet has to send an S-ACK acknowledgement packet back to the node that is two hops away from it in opposite direction.

Fig 3 shows the operational details of S-ACK mode. Source node S transfers data packet to destination node D. Consider the three consecutive nodes (say A, B, and C) as intermediate nodes in the path from S to D. These nodes work collaboratively to detect the misbehaving nodes in the network.

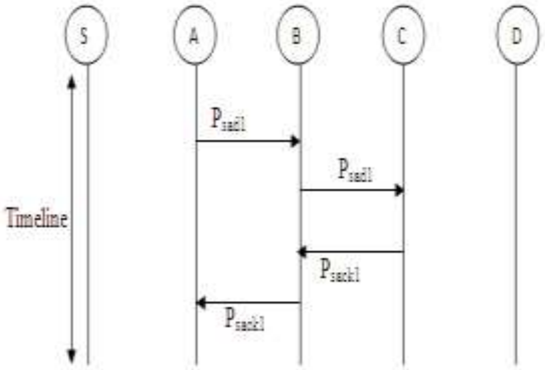


Fig 3: S-ACK mode

Node A forwards the S-ACK data packet P_{sad1} to the node B, Node B in turn forwards the same to node C. As node C is the third node in the triplet, on successful reception of this SACK packet, the node C now needs to send the S-ACK acknowledgement packet P_{sack1} back to the first node in the triplet in an opposite direction. If the first node in the triplet does not receive the S-ACK acknowledgement packet P_{sack1} in the predefined time period node A reports both B and C as malicious nodes. Therefore node A generates a misbehavior report and sends to node S which is source node.

The difference between TWOACK [15] scheme and S-ACK scheme is that in the former a source node trusts the misbehavior report even in case of report being a false one. Whereas in proposed scheme the source node on receipt of misbehavior report switches to MRA mode, and verifies if the received misbehavior report is true or false. The S-ACK scheme was introduced in order to detect the misbehaving nodes even in the presence of receiver collisions or limited transmission power.

3) MRA

When a node sends a misbehavior report regarding any other node, it is necessary to know whether the reporting node is a trusted node. The false misbehavior reports are the ones which are generated by malicious nodes in order to falsely report the innocent node as a malicious node. When a node sends a false misbehavior report to the source node indicating loss of some packet, the source node instead of trusting this report sends an MRA [13] packet via some alternative path to the destination.

This alternative route is chosen from its local knowledge base, if the alternative path is not available Energy based Geographic Routing is used to determine new route between source and destination. The destination node now compares the packet ID mentioned in MRA packet and the packet IDs of its local knowledge base. If a match is found it, then the destination node acknowledges back the source node indicating that the packet said to be lost is actually received by it. Otherwise the source will conclude that the report received is a false one and hence marks the reporter as the malicious node.

C. Batch processing

In ACK Scheme, for every packet there was an acknowledgement generated. This increases the network traffic and causes overhead. Hence batch processing is done to reduce the network overhead. For every pre-defined number of packets one acknowledgement is generated.

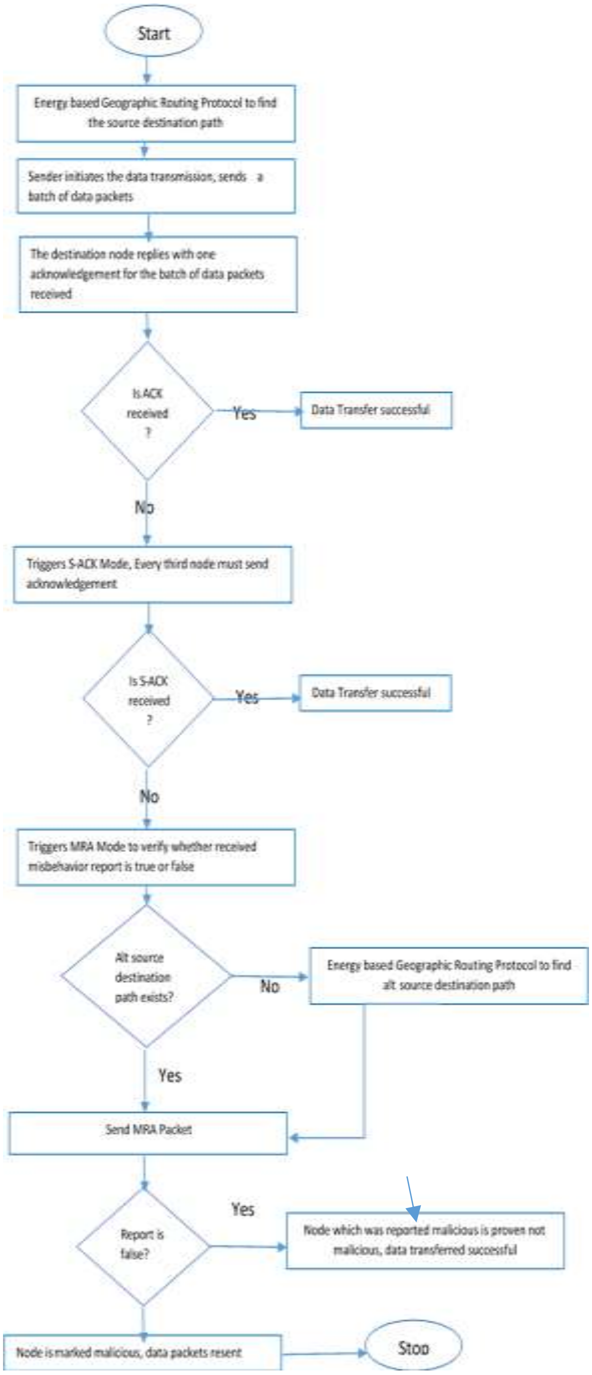
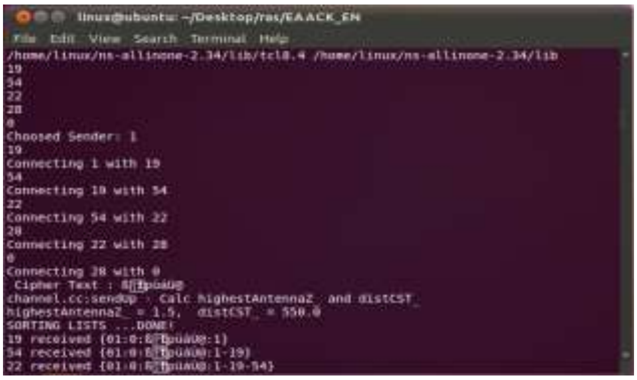

Start
Energy based Geographic Routing Protocol to find the source destination path
Sender initiates the data transmission, sends a batch of data packets
The destination node replies with one acknowledgement for the batch of data packets received
Is ACK received ?
Yes
Data Transfer successful
No
Triggers S-ACK Mode, Every third node must send acknowledgement
Is S-ACK received ?
Yes
Data Transfer successful
No
Triggers MRA Mode to verify whether received misbehavior report is true or false
Alt source destination path exists?
No
Energy based Geographic Routing Protocol to find alt source destination path
Yes
Send MRA Packet
Report is false?
Yes
Node which was reported malicious is proven not malicious, data transferred successful
Node is marked malicious, data packets resent
Stop

Fig 4: Flowchart of operational details of RIDM components

IV. IMPLEMENTATION RESULTS

The simulation of the proposed system is carried out in the Network Simulator 2 (NS2), with GCC and Ubuntu.


linux@ubuntu: ~/Desktop/ns/EAACK_EN
File Edit View Search Terminal Help

```
/home/linux/ns-allinone-2.34/lib/tcl8.4 /home/linux/ns-allinone-2.34/lib
19
54
22
28
0
Choosed Sender: 1
19
Connecting 1 with 19
54
Connecting 19 with 54
22
Connecting 54 with 22
28
Connecting 22 with 28
0
Connecting 28 with 0
 Cipher Text : [illegible]
channel.cc:sendUp - Calc highestAntennaZ_ and distCST_
highestAntennaZ_ = 1.5,  distCST_ = 550.0
SORTING LISTS ...DONE!
19 received {01:0:[illegible]:1}
54 received {01:0:[illegible]:1-19}
22 received {01:0:[illegible]:1-19-54}
```

Fig 5: Route Discovery and packet forwarding

Fig 6: Data Transfer

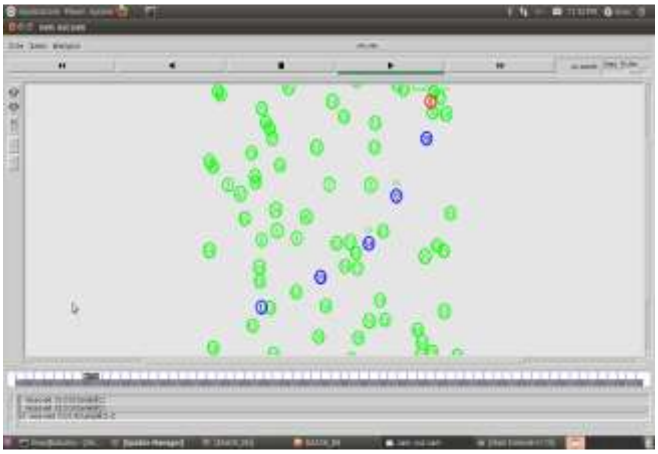


Fig 7: SACK mode

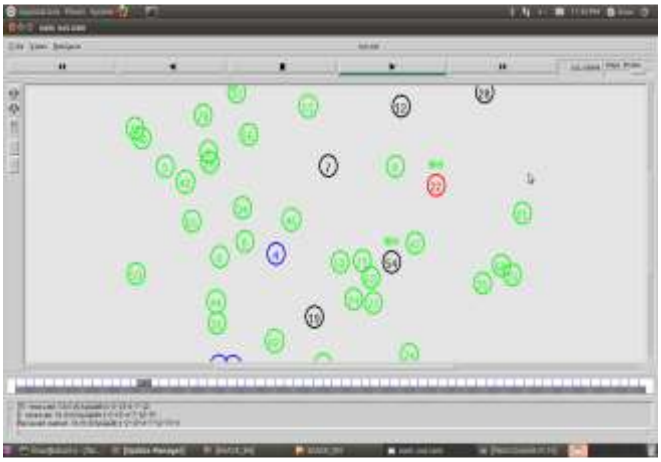


Fig 8: MRA Mode

A. Packet Delivery Ratio

The ratio of number of packets received at the destination node to the number of packets sent at the source node.

$$PDR=\frac{\mathit{Number\ of\ packets\ received}}{\mathit{Number\ of\ packets\ sent}}$$

The figure below shows the PDR comparison of both EAACK and RIDM and PDR is high in case of RIDM compared to EAACK. It can be observed that the packet delivery ratio increases as the number of nodes increases as there are more routing choices. Also as the energy of the node is also considered while routing there are no chances of a packet getting dropped due to battery drain off.

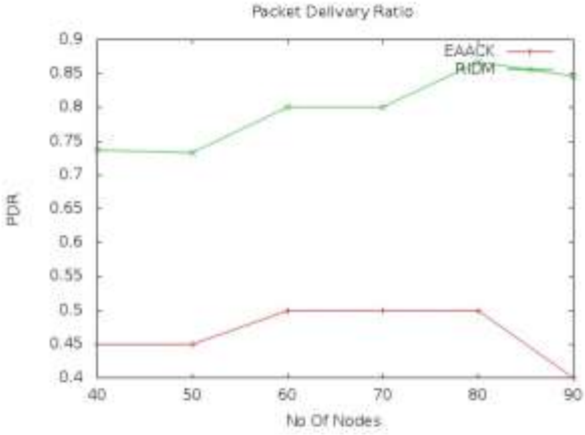


Fig 9: Packet Delivery Ratio

B.Packets Lost

The number of packets lost during the session.

Packet Lost= Number of packets sent – Number of Packets received

As the greedy forwarding technique, and energy level of each node is considered in this paper, the number of packets being dropped is reduced and hence packets lost in case of RIDM is less when compared to EAACK.

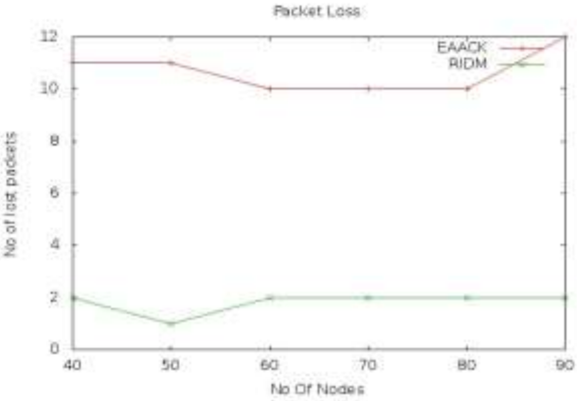


Fig 10: Packets Lost

C. Routing Overhead

RO defines the ratio of routing related transmissions like ACK, SACK, and MRA etc. The figure below shows the graph of Routing Overhead and the comparison of RO of EAACK versus RO of RIDM.

It can be observed that there is very less network overhead in case of RIDM when compared to EAACK due to the adoption of Geographic Routing Protocol and Batch processing as it reduces number of acknowledgement packets.

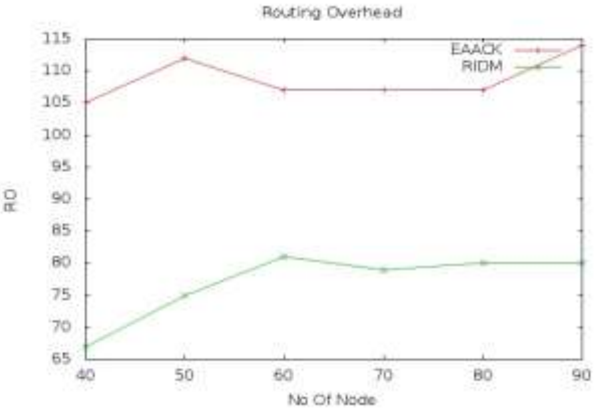


Fig 11: Routing Overhead

V. CONCLUSION

Packet-dropping attack has always been a major threat to the security in MANETs. The energy based geographic routing protocol used in this paper reduces the network overhead and also greatly improves the Packet delivery ratio as the energy of the node in Joules is also considered during selection of node in determining the path.

Similarly batch processing used reduces the number of acknowledgements.

This research work successfully improves the Packet Delivery Ratio even in case of false misbehavior attacks. The Energy based GRP used here helps the mobile nodes from draining their battery and the batch processing used here reduces the network overhead.

To increase the merits of this work, we plan to investigate the following issues in our future research:

1) Testing the performance of RIDM in real network environment.

REFERENCES

[1] H. Miranda and L. Rodrigues, ―Preventing Selfishness in Open Mobile Ad Hoc Networks,‖ *Proc. Seventh CaberNet Radicals Workshop*, Oct. 2002.

[2] L. Buttyan and J.-P. Hubaux, ―Enforcing Service Availability in Mobile Ad-Hoc WANs,‖ *Proc. MobiHoc*, Aug. 2000.

[3] Ms. Soumya Sara Zachariah, Ms. Preetha K G, "Shortest Path Geographic Routing Protocol for Mobile Adhoc NETworks", IJCSET.

[4] J.-P. Hubaux, T. Gross, J.-Y. LeBoudec, and M. Vetterli, ―Toward Self-Organized Mobile Ad Hoc Networks: The Terminodes Project,‖ *IEEE Comm. Magazine*, Jan. 2001.

[5] L. Buttyan and J.-P. Hubaux, ―Stimulating Cooperation in Self-Organizing Mobile Ad Hoc Networks,‖ *ACM/Kluwer Mobile Networks and Applications*, vol. 8, no. 5, 2003.

[6] M. Jakobsson, J.-P. Hubaux, and L. Buttyan, ―A Micropayment Scheme Encouraging Collaboration in Multi-Hop Cellular Networks,‖ *Proc. Financial Cryptography Conf.*, Jan. 2003.

[7] S. Marti, T. Giuli, K. Lai, and M. Baker, ―Mitigating Routing Misbehavior in Mobile Ad Hoc Networks,‖ *Proc. MobiCom*, Aug. 2000.

[8] J.-S. Lee, "A Petri net design of command filters for semiautonomous mobile sensor networks," *IEEE Trans. Ind. Electron.*, vol. 55, no. 4, pp. 1835–1841, Apr. 2008.

[9] J. Parker, J. Undercoffer, J. Pinkston, and A. Joshi, "On intrusion detection and response for mobile ad hoc networks," in *Proc. IEEE Int. Conf. Perform., Comput., Commun.*, 2004, pp. 747–752.

[10] A. Patcha and A. Mishra, "Collaborative security architecture for black hole attack prevention in mobile ad hoc networks," in *Proc. Radio Wireless Conf.*, 2003, pp. 75–78.

[11] T. Sheltami, A. Al-Roubaiey, E. Shakshuki, and A. Mahmoud, "Video transmission enhancement in presence ofmisbehaving nodes inMANETs," *Int. J. Multimedia Syst.*, vol. 15, no. 5, pp. 273–282, Oct. 2009.

[12] Sergio Marti, T. J. Giuli, Kevin Lai, and Mary Baker. Mitigating routing misbehavior in mobile ad hoc networks. In Mo- biCom '00: Proceedings of the 6th annual international conference on Mobile computing and networking, pages 255_265, New York, NY, USA, 2000. ACM.

[13] Elhadi M. Shakshuki, *Senior Member, IEEE*, Nan Kang, and Tarek R. Sheltami, *Member, IEEE,* EAACK—A Secure Intrusion-Detection System for MANETs IEEE TRANSACTIONS ON INDUSTRIAL ELECTRONICS, VOL. 60, NO. 3, MARCH 2013

[14] K. Liu, J. Deng, P. K. Varshney, and K. Balakrishnan, "An acknowledgment-based approach for the detection of routing misbehavior in MANETs," *IEEE Trans. Mobile Comput.*, vol. 6, no. 5, pp. 536–550, May 2007.

[15] K. Balakrishnan, J. Deng, and P.K. Varshney, ―TWOACK: Preventing Selfishness in Mobile Ad Hoc Networks,‖ *Proc. IEEE Wireless Comm. and Networking Conf*. (WCNC '05), Mar. 2005.

[16] Ms. Rasagna Chinthireddy & Dr. S Aravind, "A Survey and Comparison of Intrusion Detection Systems in MANETS" , IJETTCS,Page 58 to 64, Volume 3, Issue 3, May 2014