IJCSN International Journal of Computer Science and Network, Volume 4, Issue 1, February 2015
ISSN (Online) : 2277-5420 www.IJCSN.org
Impact Factor: 0.417

E2ACK: Preventing Routing Misbehavior in Mobile Ad hoc Networks Using OLSR Protocol

[1] Farha Nausheen, [2] Sayyada Hajera Begum

[1] Dept of IT, Muffakham Jah College of Engg. & Tech,
Hyderabad, Telangana, India

[2] Dept of IT, Muffakham Jah College of Engg. & Tech,
Hyderabad, Telangana, India

Abstract - The network topology of MANETs changes rapidly and unpredictably and due to the changing topology packet loss is a common phenomenon. Routing protocols used in MANETs are based on the assumption that, all participating nodes will be fully cooperative. But, due to the open structure node misbehavior may exist and packet loss occurs. Among them one type of misbehavior is that some nodes will take part in route establishment processes but they do not respond to forward data packets and simply dismiss the packets. The 2ACK scheme has a higher routing overhead which is caused by the transmission of 2ACK packets. So by reducing the acknowledgment ratio, Rack, the number of 2ACK transmissions can be significantly lowered. The ENHANCED 2ACK scheme is immune to the limited overhearing range issue caused due to low transmission power in the communication link. It solves the problem of ambiguous collisions, receiver collisions, and limited transmission power.

Keyword - *MANET, OLSR Protocol, 2ACK scheme, Enhanced-2ACK.*

1. Introduction

Mobile Ad-hoc Networks is a network without the aid of any fixed infrastructure, in which nodes belonging to the MANET can either act as end-points or routers. This kind of network, which is self-organizing, is very useful when the fixed infrastructure is not economically practical or physically possible such as battlefield scenarios, natural disasters, and etc. Some of the main features of MANET are [1]: MANET can be formed without any pre-existing infrastructure. It follows dynamic topology where nodes may join and leave the network at any time and the multi-hop routing may keep changing as nodes join and depart from the network. It does have very limited physical security, and thus increasing security is a major concern. Every node in the MANET can assist in routing of packets in the network, limited bandwidth and limited power. Applications of MANET with the increase of portable devices as well as progress in wireless communication, Adhoc networking is gaining importance with the increasing number of widespread applications [1]. Typical applications include: Military battlefield. Military equipment now routinely contains some sort of computer equipment. Ad hoc networking would allow the military to take advantage of common place network technology to maintain an information network between the soldier's vehicles, and military information to head quarters. The basic techniques of Ad-hoc network came from Commercial sector. Ad-hoc can be used in emergency/rescue operations for disaster relief efforts, e.g. in fire, flood, or earthquake. Emergency rescue operations must take place where non-existing or damaged communications infrastructure and rapid deployment of a communication network is needed. Local level Ad hoc networks can autonomously link an instant and temporary multimedia network using notebook computers or laptop computers to spread and share information among participants e.g. conference or classroom. Personal Area Network (PAN). Short-range MANET can simplify the intercommunication between various mobile devices (such as a PDA, a laptop, and a cellular phone).

OLSR is the table driven, proactive routing protocol designed for mobile ad-hoc networks. It exchanges routing information periodically and has route immediately available when needed. The OLSR protocol achieves optimization by determining for each node of the network a minimal subset of neighbors, called Multi Point Relays (MPR) which is able to reach all 2-hop neighbors of the node [16]. The OLSR operation can be summarized with Neighbor sensing: To achieve that each node broadcasts to its 1-hop neighbors HELLO messages periodically. MPR selection: There are two types of sets one is MPR set this set of selected neighbor nodes for each node from its 1-hop neighbors. When a node sends a routing message, only the nodes that are in its MPR set forward this message and secondly MPR selector set. Each node also maintains information about

the set of neighbors that selected it as MPR which is called MPR selector set. Each node in OLSR protocol has two tasks. First one is, correctly generate the routing protocol control traffic and second one is correctly relay the routing protocol control traffic on behalf of other nodes. Hello And Topology Control Messages Transmission OLSR nodes become aware of 1-hop and 2-hop neighbours by continuously exchanging HELLO messages with their 1-hop neighbours. MPR nodes are selected by each node in the network (called MPR Selector) as the minimum set of 1-hop neighbours that allow reaching every 2-hop neighbour via a node in the MPR set. MPR nodes optimize broadcasting and support path calculation. MPRs are the only nodes generating Topology Control (TC) messages and are also responsible for forwarding them. TC messages advertise the links between MPRs and MPR Selectors.

The shortest path algorithm uses these links to construct paths for every MPR Selector [17]. MPR selection process is as follows. MPR Selection forms the core optimization in OLSR. The idea of MPRs is to minimize the overhead of flooding messages in the network by reducing the number of redundant retransmissions. Each node in the network selects a minimum set of nodes in its symmetric, 1-hop neighbourhood which retransmit its messages. This set is selected such that every symmetric 2-hop node can be reached via a node in this set. MPR set of selected neighbour nodes is called the MPR set of that node. The neighbours of the node which are not in its MPR set, receive and process broadcast messages but do not forward them. The smaller a MPR set, the lesser the control traffic overhead of the routing protocol [17].

2. Related Work

Routing protocols for MANETs are designed based on the assumption that all participating nodes are fully cooperative. Misbehaving nodes can be significant problem. The security problem and the misbehaviour problem of wireless networks including MANETs have been studied by many researchers. Various techniques have been proposed to prevent selfishness in MANETs. These schemes can be broadly classified into two categories: credit-based schemes and reputation based schemes.

2.1 Credit-Based Schemes

The basic idea of credit-based schemes presented [5] is to provide incentives for nodes to faithfully perform networking functions. In order to achieve this goal, virtual (electronic) currency or similar payment system may be set up. Nodes get paid for providing services to other nodes. When they request other nodes to help them for packet forwarding, they use the same payment system to pay for such services. The concept of nuggets (also called beans) is used for payments for packet forwarding. And in Packet Purse Model, nuggets are loaded into the packet before it is sent. The sender puts a certain number of nuggets on the data packet to be sent. Each intermediate node earns nuggets in return for forwarding the packet. If the packet exhausts its nuggets before reaching its destination, then it is dropped. In the Packet Trade Model, each intermediate node "buys" the packet from the previous node for some nuggets and "sells" it to the next node for more nuggets. Thus, each intermediate node earns some nuggets for providing the forwarding service and the overall cost of sending the packet is borne by the destination.

2.2 Reputation-Based Schemes

The second category of techniques to combat node misbehavior in MANETs is reputation-based presented by [4]. In such schemes, network nodes collectively detect and declare the misbehavior of a suspicious node. Such a declaration is then propagated throughout the network so that the misbehaving node will be cut off from the rest of the network. The two modules under this category are watchdog and path rater. Nodes operate in a promiscuous mode where in the watchdog module overhears the medium to check whether the next-hop node faithfully forwards the packet. At the same time, it maintains a buffer of recently sent packets. A data packet is cleared from the buffer when the watchdog overhears the same packet being forwarded by the next-hop node over the medium. If a data packet remains in the buffer for too long, the watchdog module accuses the next hop neighbor of misbehaving. Thus, the watchdog enables misbehavior detection at the forwarding level as well as the link level. Based on the watchdog's accusations, the path rater module rates every path in its cache and subsequently chooses the path that best avoids misbehaving nodes. Due to its reliance on overhearing, however, the watchdog technique may fail to detect misbehavior or raise false alarms in the presence of ambiguous collisions, receiver collisions, and limited transmission power.

The CONFIDANT protocol [6] is another example of reputation-based schemes. The protocol is based on selective altruism and utilitarianism, thus making misbehavior unattractive. CONFIDANT consists of four important components—the Monitor, the Reputation System, the Path Manager, and the Trust Manager. They perform the vital functions of neighborhood watching, node rating, path rating, and sending and receiving alarm messages, respectively. Each node continuously monitors the behavior of its first-hop neighbors. If a suspicious event is detected, details of the event are passed to the Reputation System. Depending on how significant and how frequent the event is, the Reputation. System modifies the rating of the suspected node. Once the rating of a node becomes intolerable, control is passed to the Path Manager, which accordingly controls the route cache. Warning messages are propagated to other nodes in the form of an Alarm

message sent out by the Trust Manager. The Monitor component in the CONFIDANT scheme observes the next hop neighbor's behavior using the overhearing technique. This causes the scheme to suffer from the same problems as the watchdog scheme.

2.3 End-To-End Acknowledgment Schemes

There are several schemes that use end-to-end acknowledgments (ACKs) to detect routing misbehavior or malicious nodes in wireless networks. Such acknowledgments are sent by the end receiver to notify the sender about the reception of data packets up to some locations of the continuous data stream. The Selective Acknowledgment (SACK) technique [7] is used to acknowledge out-of-order data blocks.

2.4 The Twoack and S-Twoack Schemes

The TWOACK scheme was proposed in [4]. The 2ACK and the TWOACK schemes have the some major differences: The receiving node in the 2ACK scheme only sends 2ACKpackets for a fraction of received data packets, while in the TWOACK scheme TWOACK packets are sent for every data packet received. Acknowledging a fraction of received data packets gives the 2ACK scheme better performance with respect to routing overhead. The Selective TWOACK (S-TWOACK) scheme proposed in [4] is different from 2ACKas well. Mainly, each TWOACK packet in the S-TWOACK scheme acknowledges the receipt of a number of data packets, but a 2ACK packet in the 2ACK scheme only acknowledges one data packet. With such a subtle change, the 2ACK scheme has an easier control over the tradeoff between the performance of the network and the cost as compared to the S-TWOACK scheme.

4.Proposed Method

The objective of this paper is to (a). depict ENHANCED-2ACK perform better in the presence of misbehaving nodes. (b). To implement the comparison of ENHANCED-2ACK, with previously proposed acknowledge based schemes, based on criteria of detection of malicious link or node and number of acknowledgement packets transmitted, with the increase in number of nodes (i.e. 1,2….n) on active route. To obtain the results we used NS2 simulator, an Open-source event-driven simulator designed specifically for research in computer communication network. It has gained popularity in the networking research community due to its flexibility and modularity. The NS2 has strong Community base with constant revision and additions of support for new function protocols.

The present work implements an efficient system for the Enhanced 2ACK Scheme to prevent routing misbehaviour using OLSR Protocol. The implemented project work finds efficient usage under limited transmission power, limited overhearing range, routing overhead, and acknowledgement scheme. The additional routing overhead is caused by the transmission of 2ACK packets. So by reducing the acknowledgment ratio, Rack, the number of 2ACK transmissions can be significantly lowered overhead.

Routing misbehavior detection has various parameters to evaluate the performance. The biggest challenge is to find out the packet delivery ratio. Few parameters will enable us to know the performance of the ENHANCED-2ACK. Following terminologies are used for evaluation of 2ACK.

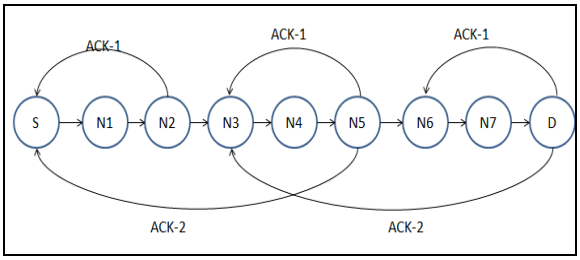

Fig 1. Block Diagram of the Implemented Design

Proposed approach as shown in Fig 2 includes the three steps, one is Detection of malicious group: Before identifying malicious or misbehaving node, network should be aware that some malicious activity is present or not. Suppose S→N1→N2→N3→N4→N5→N6→N7→D be the active route discovered. As route is discovered, source node S will form N number of sets and each set consists of three consecutive nodes (i.e. LNode, MNode and RNode respectively). LNode and RNode of any set act as temporary source and temporary destination. After forwarding data packet to next hop along the active route, each LNode makes an entry of forwarded data packet in LIST and then waits for two acknowledgement packets (i.e. ACK-1, ACK-2).

If any ACK-1 or ACK-2 packet is not received within their time limit T1 and T2 respectively, that group is considered as malicious group. Secondly, identification of particular misbehaving node: If ACK-1 is received within time T1 then LNode waits for ACK-2 else observes its MNode by rating the behavior in promiscuous mode and if rating falls threshold TS, LNode declares its MNode as misbehaving nodes and if not, LNode declares its RNode as misbehaving nodes and then flood this information.

If ACK-2 is not received within time T2, then after time T2 both MNode of that group starts rating their next hop nodes (i.e. RNode) for time T3 and when it is found that number of dropped packets exceeds threshold TS within time T3

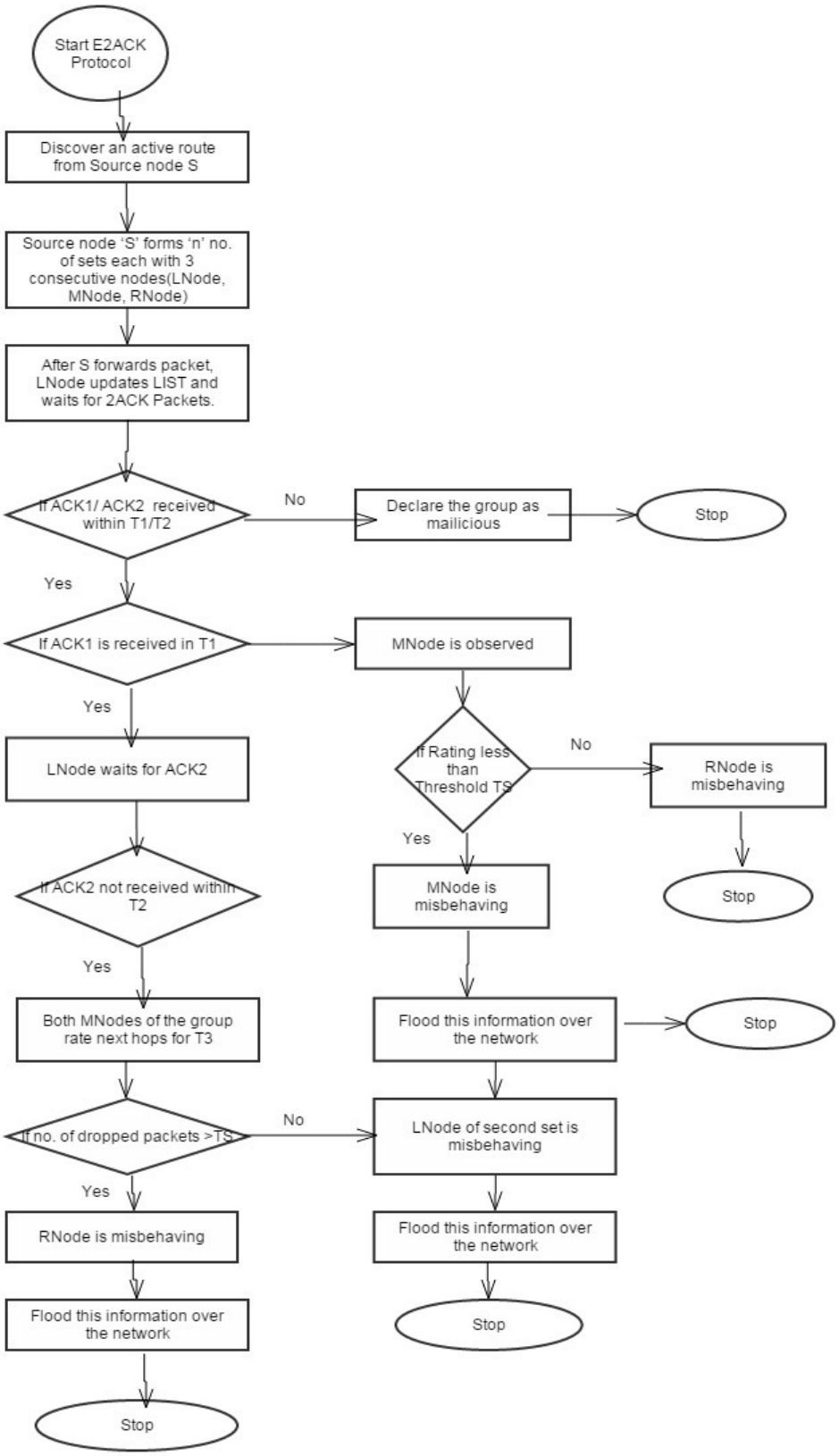

Fig. 2 System Flowchart

then that RNode is declared as misbehaving node otherwise LNode of second set is declared as misbehaving node. Finally information of misbehaving node is flooded across the network. Thirdly, isolation and mitigation of misbehaving node: Each node of network maintains a LIST of misbehaving nodes. Thus upon receiving information of misbehaving nodes, each node update their LIST and avoid using detected misbehaving node for time T4. With the expiration of time T4, the entry of misbehaving node is temporarily deleted from the LIST thereby giving a chance to previously declared misbehaving nodes to be used by network again and if the same node is caught as misbehaving node more than certain number of time (i.e. TS1) then that node is permanently isolated from network.

In order to minimize additional routing overhead due to transmission of acknowledgement packets, a fraction of data packets will be acknowledged via a single acknowledgement packet. We refer this fraction of data packets as Frank.

DataPktSrc ID	Data PktDst ID Data Pkt ID	Data PktDst ID Data Pkt ID

Fig.3 Data structure of FRANK

ENHANCED-2ACK has lesser routing overhead and more advantageous than previous similar acknowledgement based schemes as it requires lesser number of acknowledgement packet transmission.

5. Results

Routing Misbehavior detection has various parameters to evaluate the performance. The biggest challenge is to find out the packet delivery ratio. Few parameters will enable us to know the performance of the ENHANCED-2ACK. Following terminologies are used for evaluation of 2ACK.

a. Packet Delivery Ratio (PDR): Packet delivery ratio is defined as the ratio of data packets received by the destinations to those generated by the sources. This performance metric gives us an idea of how well the protocol is performing in terms of packet delivery at different speeds using different traffic models

b. Data Packet Drop: Data packet drop can be defined as number of data packet dropped by the nodes while forwarding the packets to destination. This performance metric gives us an idea how well the proposed technique is to deliver the data packet to destination.

c. Throughput: Throughput is the average rate of successful packet delivery through nodes in presence of misbehaving nodes and without presence of misbehaving nodes.

d. Routing overhead: Ratio decreased in the case of OLSR. The routing overhead is calculated by using the formula as given HELLO + TC/CBR.

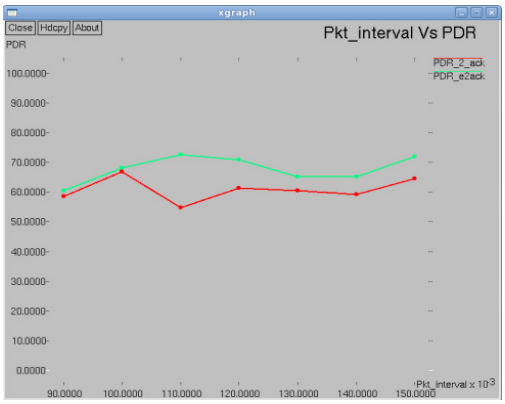

Fig 4. Pkt interval Vs. PDR Enhenced 2ACK

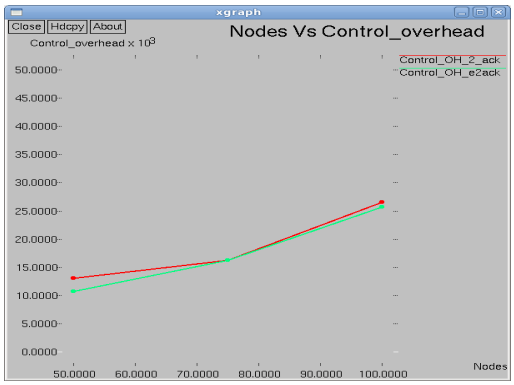

Fig 5.Nodes Vs Control Overhead

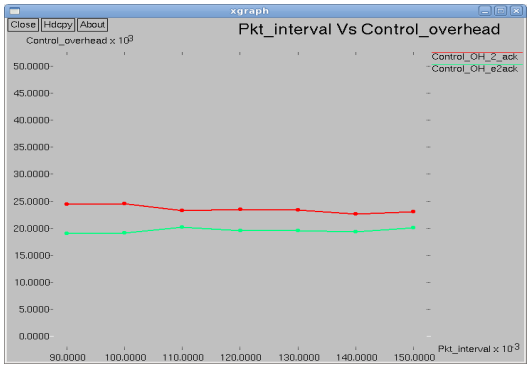

Fig 6.Pkt interval Vs Control Overhead

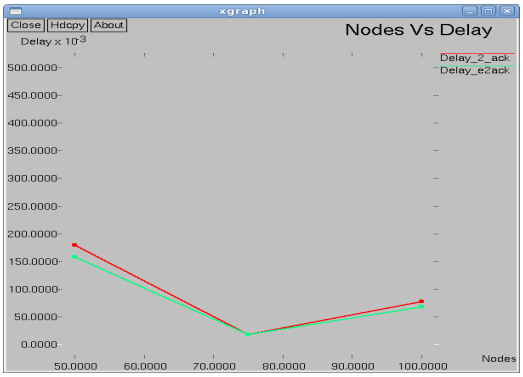

Fig.7. Nodes Vs Delay in Enhanced 2Ack

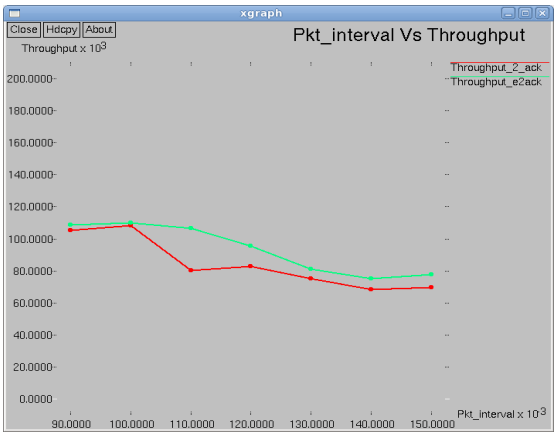

Fig.8: Throughput

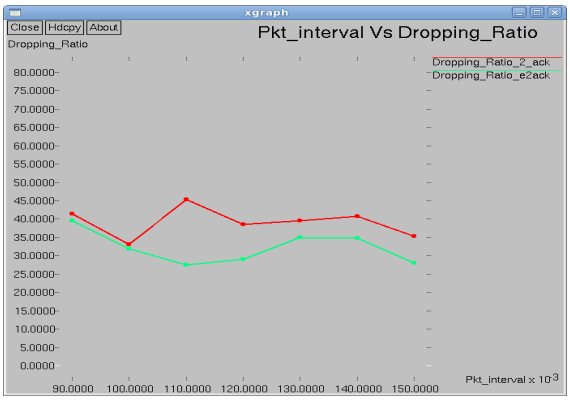

Fig.9: Dropping Ratio

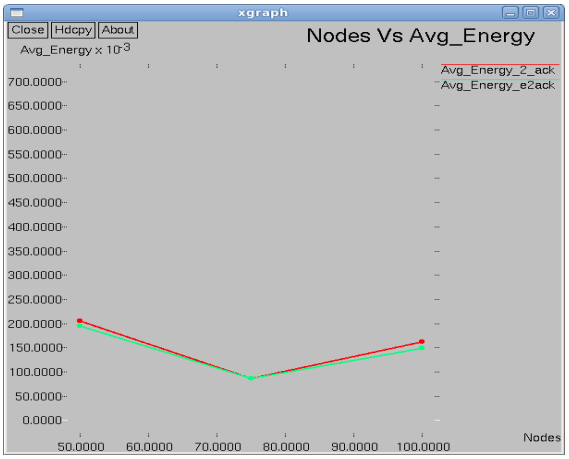

Fig.10: Average Energy in E2Ack

6. Conclusion

This paper presents ENHANCED-2ACK perform better in the presence of misbehaving nodes. Also it is proved that ENHANCED2ACK has lesser routing overhead and more advantageous than previous similar acknowledgement based schemes as it requires lesser number of acknowledgement packet transmission. It shows the comparison of ENHANCED-2ACK, with previously proposed acknowledgement based schemes, based on criteria of detection of malicious link or node and number of acknowledgement packets transmitted, with the increase in number of nodes on active route.

References

[1] Kapang Lego, Kapang Lego, DipankarSutradhar "Comparative Study of Ad-hoc Routing Protocol AODV,DSR and DSDV in Mobile Ad-hoc NETwork" Indian Journal of Computer Science and Engineering,2012.

[2] Vikram Desai, ShriramNatrajan, Tilman Wolf "Packet Forwarding Misbhavior Detection in Next Generation Network"IEEE 2012

[3] ShimaMohseni, Rosilah Hassan, Ahmed Patel, and RozilawatiRazali "Comparative Review Study of Reactive and Proactive Routing Protocols in MANETs"IEEE 2010

[4] Sergio Marti, T.G.Giuli,Kevin Lai, Mary Baker "Mitigating Routing Misbhavior in Mobile Ad-hoc Network"ACM 2000

[5] ButtyanL.AndHubaux J.-P., "Stimulating Cooperation in Self-Organizing Mobile Ad Hoc Networks," 2012.

[6] Buchegger S. And Le Boudec J.-Y., "Performance Analysis of the CONFIDANT Protocol: Cooperation of Nodes, Fairness in Dynamic Ad-Hoc Networks," Proc. MobiHoc, June 2012.

[7] Balakrishnan K., Deng J., and Varshney P. K., "TWOACK: Preventing Selfishnessin Mobile Ad Hoc Networks," Proc. IEEE 2005.

[8] C. Mbarushimana, and A. Shahrabi, "Comparative Study of Reactive and Proactive Routing Protocols Performance in Mobile Ad Hoc Networks," in Proc. of the 21st International Conference on Advanced Information Networking May 2007

[9] K. Liu, J. Deng, P. K. Varshney, and K. Balakrishnan, "An Acknowledgment-based Approach for the Detection of Routing Misbehavior in MANETs," IEEE Transactions on Mobile Computing.May 2007.

[10] Sheng Zhong , Jiang Chen , Yang Richard Yang , "Sprite: A Simple, Cheat-Proof, Credit-Based System for Mobile Ad-Hoc Networks" IEEE 2003

[11] S. A. Nagtilak, Prof. U.A. Mande" The Detection Of Routing Misbehavior In Mobile Ad Hoc Networks Using The 2ackScheme With Olsr Protocol" International Journal Of Computer EngineeringAnd Technology,2010

[12] Unikolsrd homepage http://www.olsr.org

[13] Sundararajan T.V.P., Dr.Shanmugam A." Performance Analysis of Selfish Node Aware Routing Protocol for Mobile Ad Hoc Networks", ICGST 2009

[14] G.MurugaBoopathi, N.Insozhan, S.Vinod "Selfish Nodes Detection Using Random 2ack In MANET" IJESE 2013

[15] U. Herberg and T. Clausen. "Security Issues in the Optimized Link State Routing Protocolversion 2 (OLSRv2)". International Journal of Network Security & Its Applications 2010

[16] D. Raffo, C. Adjih, T. Clausen, and P. Muhlethaler. "Securing OLSR using node locations". In Proceedings of 2005 European Wireless,2005.

[17] T. Clausen, P. Jacquet, A. Laouiti, P. Minet, P. Muhlethaler, A. Qayyum, and L. Viennot,"Optimized Link State Routing Protocol," Internet Engineering Task Force(IETF) draft, March, 2002.

Ms. Farha Nausheen graduated in Information Technology in 2007 from Muffakham Jah College of Engineering and Technology and did her M.Tech in Computer Science in 2012 from the same college. She is currently Asst. Professor in the Dept of IT, Muffakham Jah College of Engg. & Technology since 2008. She is a member of Association for Computer Machinery (ACM). Her areas of interest are Digital Electronics, Data Structures, and Computer Networks.

Ms. Sayyada Hajera Begum graduated in Information Technology from Muffakham Jah College of Engineering and Technology and did her M.Tech from Jawaharlal Nehru Technological University, Hyderabad. She is currently Asst. Professor in the Dept of IT, Muffakham Jah College of Engg. & Technology since 2007. She is a member of Association for Computer Machinery(ACM). Her areas of interest are Digital Electronics, Data Structures, Computer Networks.