Detection of Selfish Link using Enhanced ACK Method in MANET

Mr.Rushikesh Tupe[1] Mr.Shubham Tilekar[2] Mr.Nikhil Gaikwad[3] Mr.Swapnil Kadam[4] Prof. Pavan Kulkarni[5]

[1,2,3,4,5]Department of Computer Engineering

[1,2,3,4,5]Trinity College of Engineering & Research, Pune, Maharashtra, India

Abstract— A mobile ad hoc network consists of nodes that move arbitrarily and form dynamic topologies. Individual mobile nodes communicate with each other directly or indirectly via wireless link. The nodes may attempt to benefit from other nodes, but some nodes refuse to share its own resources. Such nodes are called selfish or misbehaving nodes. The nodes in MANET move freely and may change topology rapidly. These selfish nodes may severely affect the performance of network. Due to such type of node's structure and scarcely available battery-based energy, node misbehaviors may exist. One such routing misbehavior is that some selfish nodes will participate in the route discovery and maintenance processes but refuse to forward data packets. In this paper, the 2ACK scheme is used. The 2ACK scheme serves a technique for routing schemes to detect routing misbehavior and to mitigate their adverse effect. The main idea of the 2ACK scheme is to send two-hop acknowledgment packets in the opposite direction of the routing path. In order to reduce additional routing overhead, only a fraction of the received data packets are acknowledged in the 2ACK scheme. The evaluation of the 2ACK scheme uses the Dynamic Source Routing (DSR) protocol.

Key words: Mobile Ad Hoc Networks (MANET), Routing Misbehavior, Node Misbehavior, Network Security, Dynamic Source Routing

I. Introduction

A mobile ad hoc network (MANET) is a collection of mobile nodes (hosts) which communicate with each other via wireless links either directly or relying on other nodes as routers. The operation of MANETs does not depend on pre-existing infrastructure or base stations. Network nodes in MANETs are free to move randomly. Therefore, the network topology of a MANETs may change rapidly and unpredictably. All network activities such as discovering the topology and delivering data packets have to be executed by the nodes themselves either individually or collectively. Depending on its application, the structure of a MANET may vary from a small, static network that is highly power-constrained to a large-scale, mobile, highly dynamic network MANET.

Selfish Nodes: An individual mobile node may attempt to benefit from other nodes, but refuse to share its own resources. Such nodes are called selfish nodes or misbehaving nodes and their behavior is termed as selfishness or misbehavior. One of the major sources of energy consumption in the mobile nodes of MANET is wireless transmission. A selfish node may refuse to forward data packets for other nodes in order to conserve its own energy.

There are two techniques were introduced to detect and mitigate the effects of the routing misbehavior namely, watchdog and path rater, respectively. The watchdog technique identifies the misbehaving nodes by overhearing on the wireless medium. The path rater technique allows nodes to avoid the use of the misbehaving nodes in any future route selections. The watchdog technique is based on passive overhearing. Unfortunately, it can only determine whether or not the next-hop node sends out the data packet. The reception status of the next-hop link's receiver is usually unknown to the observer.

The nodes of a MANET are actually mobile routers that build up routes dynamically. These routers can move randomly and insert themselves automatically into dynamic wireless topologies. They perform packet forwarding using the current routing information. A path form the source to the destination, that is, a route, can be established through well-known routing protocols such as the ad hoc on-demand distance vector routing (AODV), dynamic source routing (DSR). Selfish and malicious nodes take advantage of MANET idiosyncrasies to misbehave, or attack.

II. Literature Survey

We have referred following papers to get an idea about the domain. So, the knowledge we have extracted is:

1) In this paper proposes routing misbehavior detection in MANETs using 2ACK scheme. Routing protocols for MANETs are designed based on the assumption that all participating nodes are fully cooperative. Node misbehavior may exist due to the open structure and scarcely available battery-based energy. [1]
2) In this paper In the existing system, a sender chooses an middle link to send some message to a destination, the middle link may not forward the packets to destination, it may be take long time to send packets or it may alter the contents of the packet. In MANETs, as there is no retransmission of packets once it is sent, care must be taken not to lose packets. [2]
3) In this paper, we propose an detection framework which detect the routing misbehavior in mobile ad hoc network. This paper describes two techniques such as watchdog and path rater to improve the throughput in an ad hoc network. The watchdog identifies misbehaving nodes and path rater helps routing protocol to avoid misbehaving nodes. [3]
4) In this paper trying to use limited transmission power to mislead the sender will be detected as well. When node sends a false report of other nodes and notify that they are misbehaving then malicious node could partition the network by claiming that some nodes following it in the path are also misbehaving.[4]
5) In this paper, many of the mobile nodes are lies in the network from that some nodes can be selfish behaviors. Selfishness is nothing the node will not transfer the resource to other node it use the resource for its own packet transmission only. In figure representing the mobile nodes and selfish. Here every mobile node send

the packet to the neighbor node but the selfish node not transferring the packets to the neighbor nodes. Selfish node aims to save its resources to the maximum. This type of misbehaving node discards all incoming packets except those which are destined to it.[5]

III. Proposed System

A. Algorithm

1) 2ACK Scheme algorithm:

In this the 2ACK scheme detects misbehavior through the use of a new type of acknowledgment packet, termed 2ACK. A 2ACK packet is assigned a fixed route of two hops (three nodes) in the opposite direction of the data traffic route.

Usage of this algorithm:

1) 2 ACK scheme is used for detecting misbehaving link or node in triplet.
2) In 2 ACK scheme algorithm, two nodes has to keep track of acknowledgement. To reduce number of ACK and detecting which node is exactly misbehaved in triplet, we come towards improved 2 ACK scheme.

Following cases are use in 2ACK sheme:

1) Best case:

In this case, let's assume that there is no misbehavior in triplet. Suppose time ™ is required to send packet and receive ACK between two consecutive nodes. The packet will be sent by N1 to N2 and will be forwarded by N2 to N3. Then N3 will send ACK in reverse path (i.e. N3->N2->N1) Here N2 will not send its own ACK to N1.

2) When N3 Misbehaved:

In the above case, let's consider N3 will misbehave (i.e. it will drop either packet or will not send ACK). In this case, N2 will wait for N3's ACK for time ™ and if it is not getting then N2 will send its own ACK to N1 which informs N1 that N3 is misbehaving as N1 is getting ACK of N2 and not of N3.

3) Worst Case:

Suppose N2 misbehaves (i.e. Either N2 drops the packet or it drops ACK sent by N3). In both cases N2 can't send ACK to N1 which will inform N1 after time 2TM (time starts from packet sent from N1 to N2) N2 is misbehaving.

B. System Architecture

In proposed system consist of architecture of following component Node as computer, Router as use network, Power Supply etc.

An architectural model for MANETs which preserves the integrity of the IP architecture while allowing for the particularities of MANET .An architectural model considers MANET nodes as routers with hosts attached, as however the important observation to make is, that the links between these hosts and the router are classic IP links.

This implies that, from the point of view of the hosts, and the applications on these hosts, connectivity is via a classic IP link. Hosts, and their applications, are not exposed to the specific characteristics of the MANET interfaces and are connected to the MANET via a router, which has one or more MANET interfaces.. Fig shows MANET node model: the router (R) has on the top a MANET interface, and is connected, on the bottom, to hosts (H) via classic IP links. Since the hosts in figure are connected to a classic IP link, these hosts are configured and behave as hosts in any other network, and the links to which they are connected have properties identical to those of any other classic IP link.

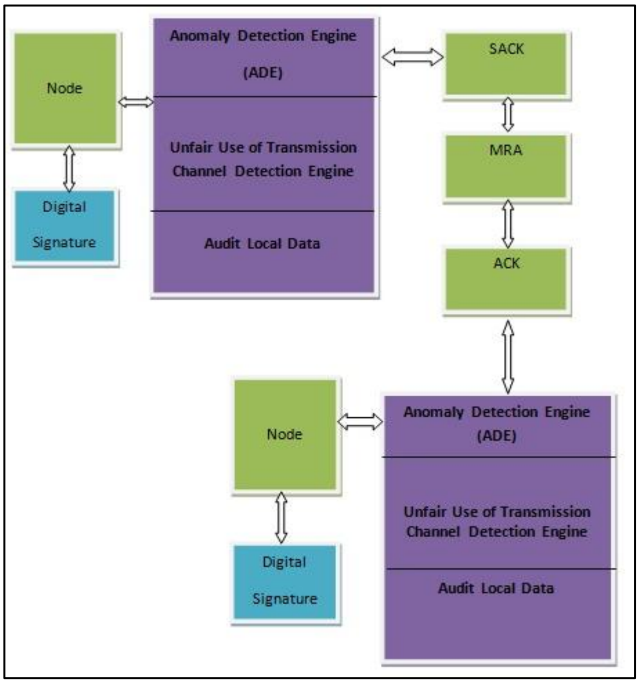

Node
Digital Signature
Anomaly Detection Engine (ADE)
Unfair Use of Transmission Channel Detection Engine
Audit Local Data
SACK
MRA
ACK
Node
Digital Signature
Anomaly Detection Engine (ADE)
Unfair Use of Transmission Channel Detection Engine
Audit Local Data

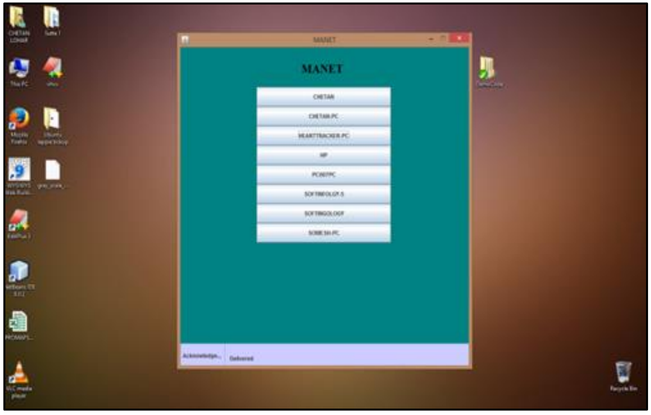
Fig. 1: Proposed System Architecture

IV. Methodology

The working of our system is given below with the help of screenshots of our system and explanation in brief manner:

A. Main GUI showing all nodes in Network.

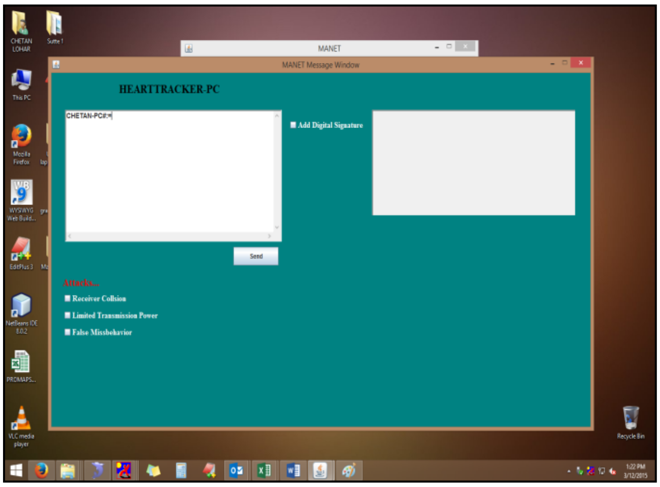
1) First we run main form.
2) The main form display on screen with showing all nodes in the network.
3) Select the receiver at these step.



Main GUI

B. Message window is open after selecting the receiver

1) In Message window we are Typing message.
2) Then click on add digital signature.
3) After you can select whatever option you want to select.
4) Then at the end click on send button.



CHETAN-PC#:=

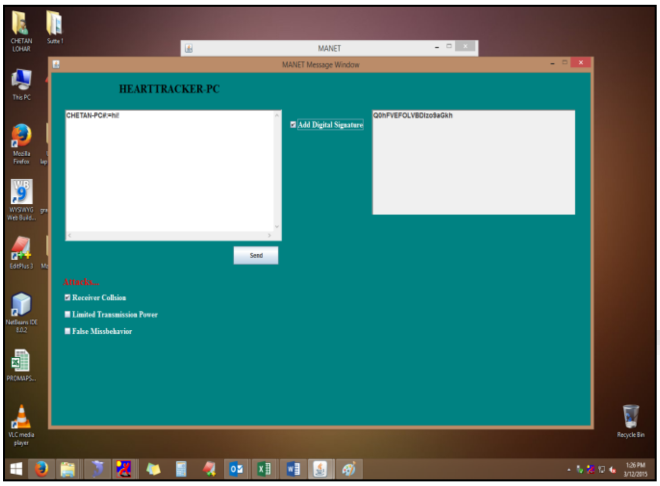
□ Add Digital Signature

□ Receiver Collsion
□ Limited Transmission Power
□ False Missbehavior

Message Window

C. *These snapshots select the Receiver Collision.*

1) For detecting the receiver collision attack we need to select the receiver collision.
2) First message forwarded window is open.
3) Then sender get the message the receiver collision is detected.



CHETAN-PC#:=hi!

☑ Add Digital Signature

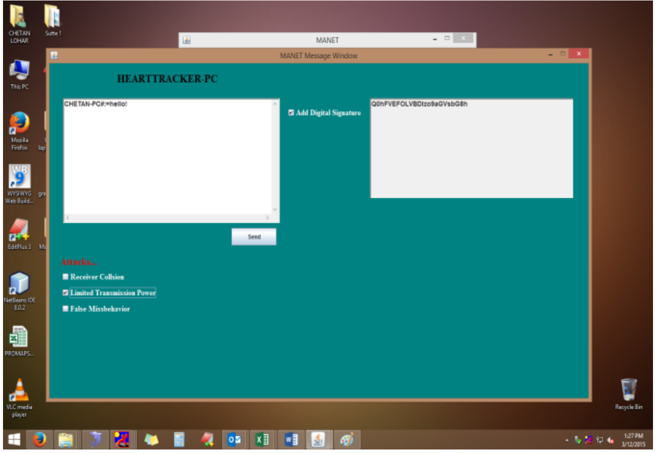
Q0hFVEFOLVBDIzo9aGkh

☑ Receiver Collsion
□ Limited Transmission Power
□ False Missbehavior

Receiver Collision attack

D. *This message window shows the limited transmission power.*

1) In these form the limited transmission power attack is check.
2) And due to the limited power attack "message is not delivered" window is open.



CHETAN-PC#:=hello!

☑ Add Digital Signature

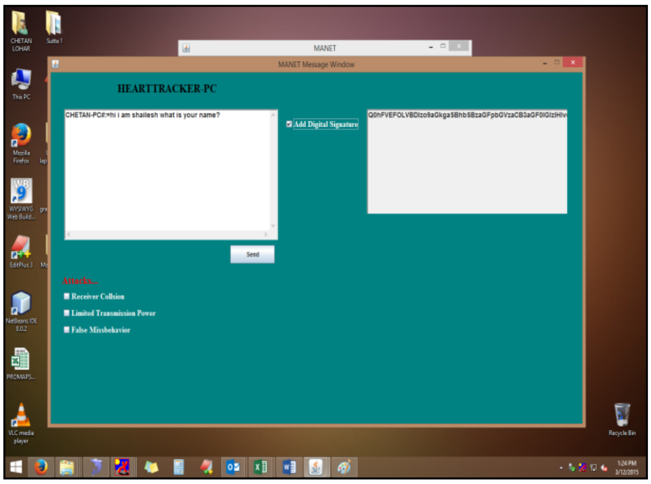
Q0hFVEFOLVBDIzo9aGVsbG8h

□ Receiver Collsion
☑ Limited Transmission Power
□ False Missbehavior

Limited Transmission Power attack.

E. *False misbehavior window*

1) In these form we are checking False misbehavior report
2) After the selecting the false misbehavior button the false misbehavior report is generated.



CHETAN-PC#:=hi i am shailesh what is your name?

☑ Add Digital Signature

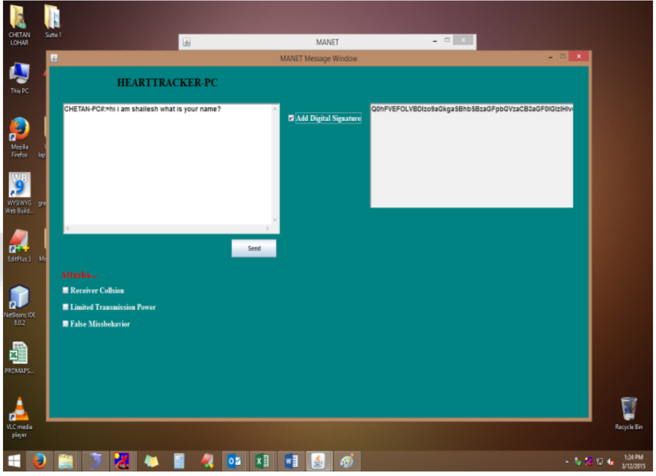
Q0hFVEFOLVBDIzo9aGkgaSBhbSBzaGFpbGVzaCB3aGF0IGlzIHlv

□ Receiver Collsion
□ Limited Transmission Power
□ False Missbehavior

False misbehavior report attack

F. *Message with Digital Signature*

These form shows the digital signature is display on the message window



CHETAN-PC#:=hi i am shailesh what is your name?

☑ Add Digital Signature

Q0hFVEFOLVBDIzo9aGkgaSBhbSBzaGFpbGVzaCB3aGF0IGlzIHlv

□ Receiver Collsion
□ Limited Transmission Power
□ False Missbehavior

Message with digital signature

G. *System Requirements*

1) *Frontend:*
   - .NetBeans
   - Database
   - Java API , JDK
2) *Backend:*
   - MySQL
3) *Hardware:*
   - Keyboard,
   - Mouse and
   - Laptop or PDA.
   - GUI developed using swings
   - Operating System : Window XP, Window Vista or 7
   - Processor : Intel Chipset
   - Memory : 2 GB
   - Hard Drive Capacity : 200GB, expandable
   - Browser: Internet Explorer 6 and above.

- Mozilla or
- Google Chrome.
- Wi-Fi Router

V. Conclusion

None of proposed security solutions has been as successful on ambiguous collision, receiver collision and on false misbehavior in wireless mobile ad-hoc network. Wireless network are low cost and easy to deploy. In our project "Detection of Selfish Link using Enhanced-ACK Method in MANET" we have used innovative IDS with digital Signature Algorithm which is capable of providing authentication and confidentiality to data which will be sent from one node to another node. Due to infrastructure less or decentralized network we have to provide additional security in terms of Intrusion Detection System for each and every node in MANET. These innovative IDS will perform to produce desired results and it helps system from preventing various types of attacks.

Acknowledgment

The project on project "Detection of Selfish Link using Enhanced-ACK Method in MANET" is a source of trending and immense information to us. We would glad to express our sincere gratitude to the Trinity College of Engineering and Research department of Computer Technology for the guidance and most valuable support in the help for this project work. We acknowledge with a pleasant gratitude, the encouragement and inspiration received from our guide Prof.Pavan Kulkarni, project coordinator Prof.Suchita Wankhede, Head of the Department Prof.Pavan Kulkarni and colleagues.

References

[1] N. Ramya ,Dr. S. Rathi," 3rd International Conference on Advanced Computing and Communication Systems (ICACCS -2016), 978-1-4673-9206-8/16/$31.00 ©2016 IEEE, Jan. 22 – 23, 2016
[2] Hernandez-orallo Et Al, "Cocowa: A Collaborative Contact-based Watchdog For Detecting Selfish Nodes" IEEE Transactions On Mobile Computing, Vol. 14, No. 6, June 2015
[3] Hern_andez-Orallo, M. D. Serrat, J.-C. Cano, C. M. T. Calafate, and P. Manzoni, "Improving selfish node detection in MANETs using a collaborative watchdog," IEEE Comm. Lett., vol. 16, no. 5, pp. 642–645, May 2012.
[4] Rasika R. Mali, Sudhir T. Bagade, "2016 International Conference on Computing, Analytics and Security Trends (CAST) College of Engineering Pune,India" 978-1-5090-1338-8/16/$31.00 ©2016 IEEE, Dec 19-21, 2016
[5] Arockia Rubi and Vairachilai, "A Survey on Intrusion Detection System in Mobile Adhoc Networks," International Journal Of Computer Science And Mobile Computing, vol. 2, issue 12, pp. 389-393, December. 2013
[6] Rasika Mali and Sudhir Bagade, "Techniques for Detection of Misbehaving Nodes in MANET: A Study," International Journal of Scientific & Engineering Research, vol. 6, Issue 8, August 2015.
[7] Hatware, A. Kathole, M. Bompilwar "Detection of Misbehaving Nodes in Ad Hoc Routing," International Journal of Emerging Technology and Advanced Engineering, vol. 2, Feb. 2012.
[8] Mangesh M Ghonge, Dr. V. M. Thakare, "International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS) Selfish Attack Detection in Mobile Ad hoc Networks",2016
[9] Aishwarya Anand S Ukey, Meenu Chawla and Virendra Pal Singh, "I-2ACK: Preventing Routing Misbehavior in Mobile Ad hoc Networks", International Journal of Computer Applications 62(12):34-39, January 2013.
[10] 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, vol. 6, no. 5, pp. 536-550, May 2007.
[11] Sunilkumar S. Manvia, Lokesh B. Bhajantrib, and Vittalkumar K. Vaggac, ' Routing Misbehavior Detection in MANETs' Using 2ACKNOWLEDGEMENT, journal of telecommunication and information technology 4/2010.