International Journal of Computer Theory and Engineering, Vol. 2, No. 5, October, 2010
1793-8201

A Highly Secured Approach against Attacks in MANETS

G.S. Mamatha and Dr. S. C. Sharma

Abstract— **One of the major reasons to address the security aspects in MANETS is the usage of wireless transmission medium, which is highly susceptible or vulnerable to attacks. This paper proposes a way to identify parallelly different types of attacks in MANETS. This approach is highly secure as it essentially concentrates on identifying misbehaving links, number of significant packets dropped and malicious nodes parallelly. This paper shows the implementation of identification and prevention of malicious nodes launching packet dropping and message tampering attacks, using a semantic security mechanism. This security scheme is highly impossible to break, thereby making it a highly secured approach. The evaluation results demonstrate that the approach effectively detects and prevents such nodes and links in networking sessions**.

Index Terms—**Attacks, Malicious nodes, MANETS, Message tampering, semantic, Packet dropping, Security.**

I. Introduction

Compared to wireless networks in infrastructure mode ad-hoc networking doesn't require any access points. This makes them useful in a lot of different applications. It is largely used in military applications and in rescue operations where the existing communication infrastructure has been destroyed or is unavailable, for example after earthquakes and other disasters. But ad-hoc is now a days also being used in a lot of commercial applications, like mobile phones and PDAs using the Bluetooth protocol, since it is fast and quite easy to setup and doesn't require any extra equipment. As MANETS (Mobile Ad hoc Networks) is quickly spreading for the property of its capability in forming temporary network without the aid of any established infrastructure or centralized administration, security challenges has become a primary concern to provide secure communication. To accomplish our goal, we have done literature survey in gathering information related to various types of attacks and solutions, as well as we have made comparative study to address the threats in different layers. Finally, we have identified an approach to tackle to a maximum extent the attacks in MANETS. In our study, we have found that necessity of secure routing protocol is still a burning question [1]. There is no general algorithm that suits well against the most commonly known attacks such as black hole, gray hole wormhole, rushing attack etc. The main idea of the paper is to propose an approach that tackles with particularly the network layer attacks. The proposed scheme uses one way hash computation which is highly impossible to be known by the malicious nodes to launch an attack. The Paper is organized as given below: In the II section background study is discussed. Section III deals with the design aspects of the approach. Section IV gives a detailed illustration of the proposed scheme. Section V gives experimental analysis for the proposed scheme. In Section VI as a conclusion, we focus on the findings and future works which may be interesting for the researchers for complete security solutions in MANETS.

Manuscript received April 8th 2009.
G.S. Mamatha, Lecturer, Information Science Department, R.V. College of Engineering, Mysore Road, Bangalore - 560059.
Dr. S. C. Sharma,Vice-Chancellor,Tumkur University,Tumkur, Karnataka.

II. Related Work

The following list of papers shows the relative work carried out for different types of attacks in MANETS and possible solutions given.

1) Detecting Network Intrusions via Sampling: A Game Theoretic Approach: In this paper, the problem of detecting an intruding packet in a communication network is considered [2].
2) A Distributed Security Scheme for Ad Hoc Networks discuss the DoS attack like flooding using AODV protocol and concludes with an immediate enhancement to make the limit-parameters adaptive in nature. This can be done by making calculations based on parameters like memory, processing capability, battery power, and average number of requests per second in the network and so on [3].
3) Wormhole attacks detection in wireless ad hoc networks using a statistical analysis approach [4].
4) Wormhole Attack Detection in Wireless Sensor Networks: This paper analyzes the nature of wormhole attack and existing methods of defending mechanism and then proposes round trip time (RTT) and neighbor numbers based wormhole detection mechanism [5].
5) A study of different types of attacks on multicast in mobile ad hoc networks: considers only rushing attack, black hole attack, neighbor attack and jellyfish attack [6].
6) Mitigating denial-of-service attacks in MANET by incentive-based packet filtering: A game-theoretic approach [7].
7) A survey of routing attacks in mobile ad hoc networks which considers only routing attacks, such as link spoofing and colluding misrelay attacks [8].
8) A Secure Routing Protocol against Byzantine Attacks for MANETs in Adversarial Environments which considers an integrated protocol called secure routing

against collusion (SRAC), in which a node makes a routing decision based on its trust of its neighboring nodes and the performance provided by them [9].

9) Enhanced Intrusion Detection System for Discovering Malicious Nodes in Mobile Ad Hoc Networks: The main feature **of** the proposed system is its ability to discover malicious nodes which can partition the network by falsely reporting other nodes as misbehaving and then proceeds to protect the network by [10].
10) Detection and Accusation of Packet Forwarding **Misbehavior** in Mobile Ad-Hoc networks using flow of conservation mechanism and done with protocol less implementation [11].
11) WAP: Wormhole Attack Prevention Algorithm in Mobile Ad Hoc Networks without using any specialized hardware wormholes can be detected and isolated within the route discovery phase [12].
12) A Reliable and Secure Framework for Detection and Isolation of Malicious Nodes in MANET: This security framework involves detection of malicious nodes by the destination node, isolation of malicious nodes by discarding the path and prevention data packets by using dispersion techniques [13].
13) A Cooperative Black hole Node Detection Mechanism for ADHOC Networks [14].
14) DPRAODV: A Dynamic learning system against black hole attack in aodv based Manet [15].

The most of the related study covers only few network layer attacks like black hole, wormhole or as a whole to identify the malicious nodes. In the proposed secured approach, we are trying to extend the approach to identify more number of network layer attacks parallelly.

III. Design

Two main approaches are used to make routing protocols handle attacks in ad hoc networks. The first approach aims at detecting the malicious nodes while computing the route in the network and re-routing the packets around it, mostly along the shortest path among them. Most of these protocols are based on existing ad hoc routing protocols like AODV [16], DSDV [17] and DSR [18], designed to handle attacks.

The design of our algorithm is almost based on first approach. The design is based on three modules. First will be the sender module, second will be the intermediate node module and third will be the receiver module. AODV (Adhoc on demand distance vector protocol) is used as data forwarding protocol. To develop our proposed system, we use the simple acknowledgement approach which has two way communications, a semantic security mechanism to generate hash code and principle of flow conservation to identify the threshold value for packet dropping.

IV. Proposed Scheme

In section II a related study on attacks has shown which indicates that most of the work is done considering only one or two network layer attacks. Since network layer is mainly used for packet forwarding, the attacks in this layer are considered. At the network layer we assume that nodes misbehave, by dropping or delaying packets despite having agreed to forward them during route discovery. And that routing is done before hand. In that way it is going to reduce the packet drop ratio and also aims at efficient data forwarding in MANETS and in that process monitors the misbehaving nodes or links, so that such nodes or links are avoided in data forwarding. We detect nodes that misbehave by launching attacks on either a single node or parallelly to more number of nodes by inducing significant delay in the packet or by altering the contents of the packets or by routing the packet to a non-destined node or by sending a packet out of transmission range or some other means. The approach can also be called highly secured in the sense that, the algorithm is capable of identifying several attacks launched by malicious nodes and there by preventing them for future sessions.

The detailed description of the implementation of the algorithm is explained as follows:

Route discovery is done in accordance with the data forwarding protocol used. In this proposed algorithm, an on demand protocol like AODV is suitable because, AODV is a hop-by-hop routing protocol, which introduces a more dynamic strategy to discover and repair route when compared to other on-demand protocols. Destination sequence numbers are used to avoid the problem of infinite loops. AODV maintains only active routes to reduce overheads and control traffic. It is suitable for scenarios with moderate mobility and density networks.

When route is ready, sender starts sending the message and divides it in to packets of 48 bytes each. Then constructs the data frame with source address, destination address, message to be sent and hash code for confidentiality purpose. A counter is kept (cpkt) to increment every time a packet has been sent. This is called one way hash chain method, which is impossible for the attacker to break. Even a small change in the data will change the hash value, which is easily identified by the receiver, since receiver also computes the same hash code. Sender then connects to the nearest intermediate node to forward the message and waits for acknowledgement. Intermediate node then extracts data frame and identifies the destination address to forward message to it. Once the data reaches destination, the data frame is extracted by the receiver node and hash code is computed to match with the hash code of sender. If hash code of destination is same as that of sender, then destination node prepares an acknowledgement frame with an "ACK" field and sends back to the sender through the same intermediate nodes. Such nodes can be called genuine nodes. Otherwise acknowledgement frame is prepared with a "CONFIDENTIALITY LOST" field and sent back to sender, which means the message sent has been tampered. In such a case, the link through which the data traversed contains malicious nodes. Once the source gets the acknowledgement from destination node, the time taken for acknowledgement to reach back the sender is calculated (end). Then RTT (Round Trip Time) is calculated by subtracting the end time with that of the start time of sending the data packet (start) as (end-start), for each of the message sent from the sender node in milliseconds.

A time limit for RTT is set to 20ms. If an

acknowledgement to reach back to the sender node is exceeding the time limit set, then it is assumed that the packets are lost. Parallelly a counter is kept (cmiss) to increment every time a packet is lost I.e. acknowledgement is exceeding 20ms. Repeat the procedure for every data frame that is sent. A ratio of (cmiss/cpkt) is calculated. To evaluate this ratio, we are using Principle of Flow Conservation mechanism [11] by setting the threshold value to this ratio as 20%, I.e. (cmiss/cpkt)<=20% (0.2), which is called the limit of tolerance. If any route chosen is exceeding this ratio is said to be misbehaving and discards the misbehaving node by choosing the next alternative node to complete the communication. If sender finds the "CONFIDENTIALITY LOST" field in the acknowledgement frame then it comes to know about the malicious node from the routing table information which has tampered the message, maintained by the sender node. Such links which exceeds limit of tolerance ratio and has the above information in their acknowledgement is discarded for further sessions.

As explained in design section, all the modules have got a front end design for appropriate message displays.

A sample snapshot in the fig 4.1 shows the front end design for the sender module.

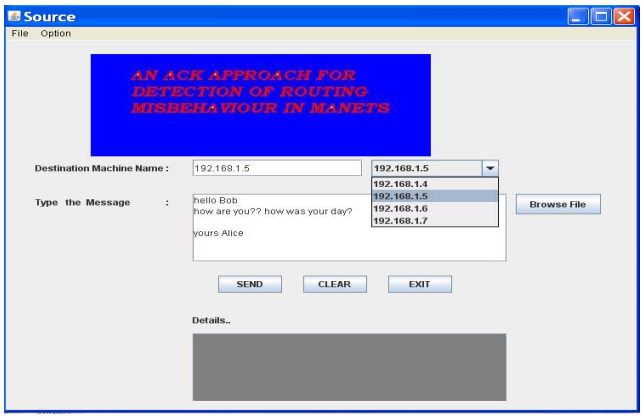

FIG: 4.1Sender module

V. Experimental Analysis

The proposed algorithm was practically implemented and tested in a lab terrain. Through the experiment analysis it is found that the algorithm exactly shows the results for two attacks namely packet dropping and message tampering. To analyze the reactive routing protocol mechanism two laptops are connected at both the ends in between 22 numbers of intermediate nodes with WI-FI connection.

The underlying MAC protocol defined by IEEE 802.11g was used with a channel data rate of 2.4 GHZ. The data packet size can vary up to 512-1024 bytes. The wireless transmission range of each node was 100 m. Traffic sources of constant bit rate (CBR) based on TCP have been used.

The evaluation has been done for about 10 to 15 messages that are sent from the sender node. For tabulation purpose we have considered only few messages and the corresponding values obtained for each case (For tabulation these messages are indicated as MSG1 to MSG5). Based on the values obtained and comparing them with the limit values, the attacks have been identified. The data transmission for all the messages sent takes place in just in few milliseconds, which saves the battery life of the nodes, thereby satisfying one important criterion of MANETS.

The same approach can be extended to few more attacks identification and prevention, which can be kept as the future enhancement. Further the node density can also be increased to test for the proposed approach and analyzed. Simulation can also be taken as another enhancement for the approach to consider more number of nodes and graphical analysis.

The following table 1 shows the results for the experiment conducted:

TABLE: 5.1 SUMMARIES OF RESULTS

Data Sent	RTT (ms)	(cmiss/ cpkt) ratio	Link Status	Node Status	Attack Identified
MSG1	16	0.0	Working properly	Genuine	nil
MSG2	10	0.014	Working properly	Genuine	nil
MSG3	16	0.0	Working Properly but CONFIDEN TI-ALITY LOST	Malicious	Message tampering
MSG4	10.47	1.0	Misbehaving	Malicious	Packet dropping
MSG5	31	1.0	Misbehaving and CONFIDEN TI-ALITY LOST	Malicious	Packet dropping, message tampering

The result screens which support the above results are as follows from fig 5.1 to fig 5.4.

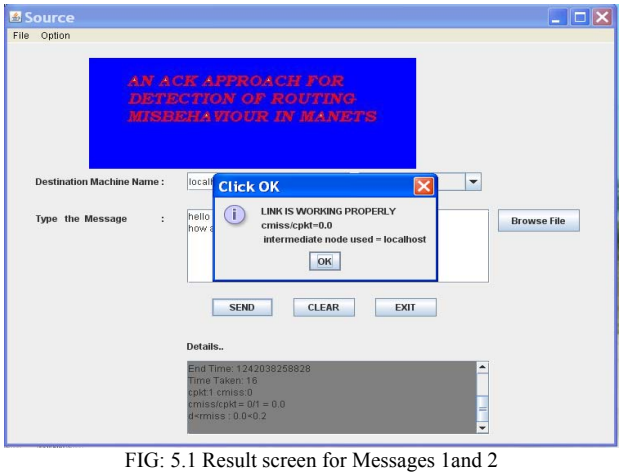

FIG: 5.1 Result screen for Messages 1and 2

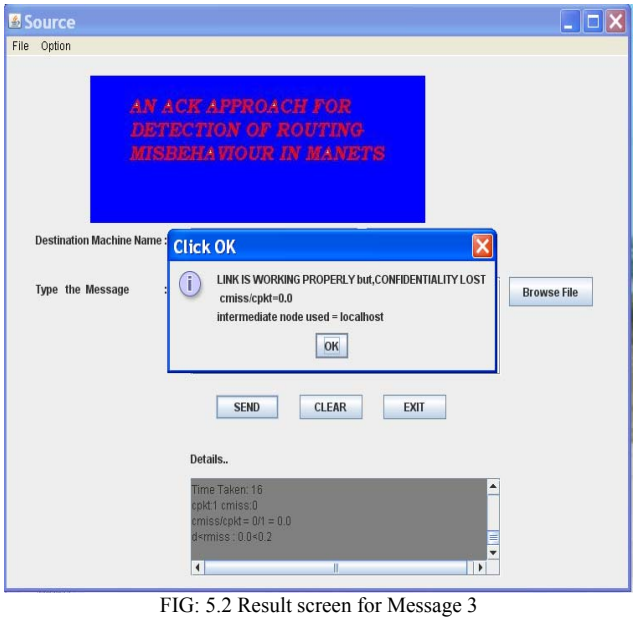

FIG: 5.2 Result screen for Message 3

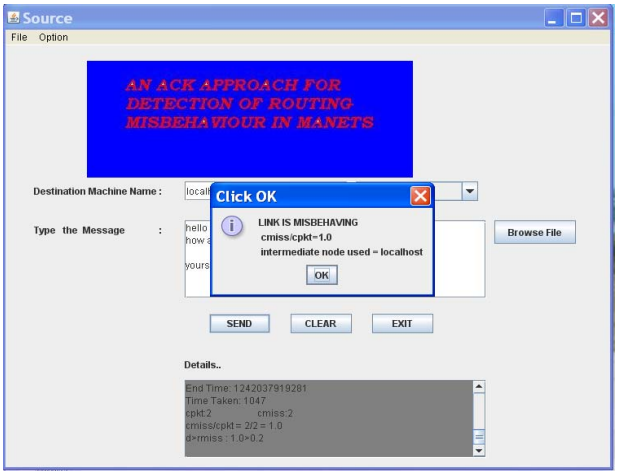

FIG: 5.3 Result Screen for Message 4

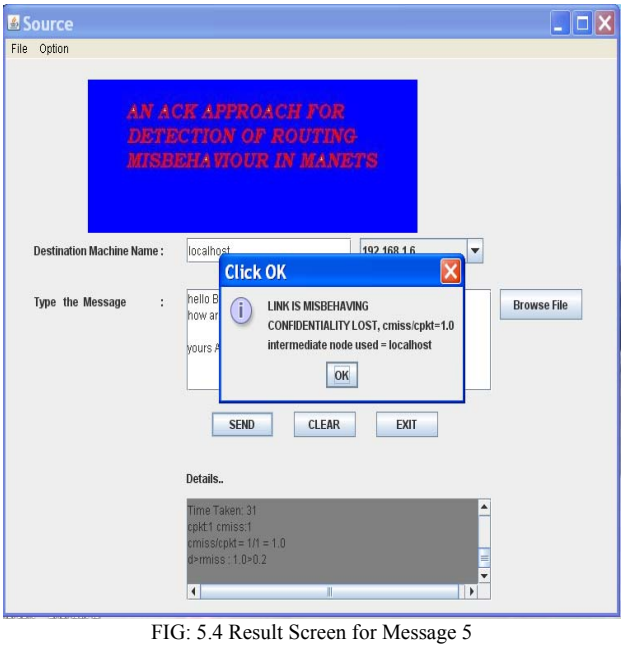

FIG: 5.4 Result Screen for Message 5

VI. Conclusion

As security is major concern in MANETS, this approach will tackle the issue in an efficient manner. Reactive methods should be used instead of proactive methods since attacks on packet forwarding cannot be prevented. The core idea of this algorithm is to detect malicious nodes launching attacks and misbehaving links to prevent them from communication network. A robust and a very simple idea is presented here which can be implemented and tested in future for more number of attacks by increasing number of nodes.

Acknowledgment

I owe my sincere feelings of gratitude to Dr. S.C. Sharma for

his valuable guidance and suggestions which helped me a lot

to write this paper. It gives us great pleasure to express my feelings of gratitude to Dr. Ramakanth Kumar and Usha. J, for their valuable guidance, support and encouragement.

References

[1] Kamanashis Biswas and Md. Ali, "Security threats in Mobile ad hoc networks", University essay from Blekinge Tek nisha Ho gskola/Sektionen for Teknik (TEK), 2007.

[2] Murali Kodialam T. V. Lakshman, "Detecting Network Intrusions via Sampling: A Game Theoretic Approach", IEEE INFOCOM, 2003.

[3] Dhaval Gada, Rajat Gogri, Punit Rathod, Zalak Dedhia and Nirali Mody Sugata Sanyal, Ajith Abraham, "A Distributed Security Scheme for Ad Hoc Networks", ACM Publications, Vol-11, Issue 1, 2004, pp. 5 – 5.

[4] N. Song, L.Qian, X. Li, "Wormhole attacks detection in wireless ad hoc networks: A statistical analysis approach", Parallel and Distributed Processing Symposium, Proceedings, 19th IEEE International, 2005.

[5] Zawtun and Aung Htein Maw, "Wormhole attack detection inwireless sensor networks", World Academy of Science, Engineering and Technology, 46, 2008.

[6] Hoang Lan Nguyen and UyenTrang Nguyen, "A study of different types of attacks on multicast in mobile ad hoc networks", IEEE proceedings in International Conference on Networking (ICN 2006), 2006.

[7] Xiaoxin Wu, David K.Y, "Mitigating denial-of-service attacks in MANET by incentive-based packet filtering: A game-theoretic approach", 3rd International conference on secureCommunications, September 2007, pp. 310-319.

[8] Kannhavong, B. Nakayama, H. Nemoto, Y. Kato, N. Jamalipour, A , "A survey of routing attacks in mobile ad hoc networks", IEEE Journal on Wireless Communication, Vol-14, Issue 5, December 2007, ISSN: 1536-1284, pp.85-91.

[9] Ming Yu; Mengchu Zhou; Wei Su, "A Secure Routing Protocol Against Byzantine Attacks for MANETs in Adversarial Environments", IEEE Transactions on Vehicular Technology Vol-58, Issue 1, Jan. 2009 , pp.449 – 460.

[10] Nasser, N.; Yunfeng Chen, "Enhanced Intrusion Detection System for Discovering Malicious Nodes in Mobile Ad Hoc Networks", IEEE International Conference on Communications, ICC apos; Vol-07 , Issue 24-28 June 2007 , pp.1154 – 1159.

[11] Oscar F. Gonzalez,God win Ansa, Michael Howarth, and George Pavlou, "Detection and Accusation of Packet Forwarding Misbehavior in Mobile Ad-Hoc networks", Journal of Internet Engineering, vol-2, 2008, pp.1.

[12] Sun choi, Doo-young Kim, Do-hyeon Lee, Jae-il Jung, "WAP: Wormhole Attack Prevention Algorithm in Mobile Ad Hoc Networks", International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing, Vol-0 , ISBN = {978-0-7695-3158-8}, 2008, pp.343-348 .

[13] S.Dhanalakshmi, Dr.M.Rajaram, "A Reliable and Secure Framework for Detection and Isolation of Malicious Nodes in MANET", IJCSNS International Journal of Computer Science and Network Security, vol-8 No.10, October, 2008.

[14] Moumita Deb, "A Cooperative Black hole Node Detection Mechanism for ADHOC Networks", Proceedings of the World Congress on Engineering and Computer Science, 2008.

[15] Payal N.Raj and Prashant B. swadas, " DPRAODV: A Dynamic learning system against blackhole attack in AODV based MANET", International Journal of Computer ScienceIssues, vol-2, 2009.
[16] Charles E. Perkins, Elizabeth M. Belding Royer and Samir R. Das, "Ad-hoc On-Demand Distance Vector (AODV) Routing", Mobile Ad-hoc Networking Working Group, Internet Draft, draft-ietf-manetaodv- 00.txt, February 2003.
[17] Charles E. Perkins and Pravin Bhagwat, "Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers", Proceedings of the SIGCOMM '94 Conference on Communications Architectures, Protocols and Applications, August 1994, pp. 234-244.
[18] D. B. Johnson, D. A. Maltz, "Dynamic Source Routing in Ad Hoc Wireless Networks", Mobile Computing, edited by Tomasz Imielinski and Hank Korth, Chapter 5, pages 153- 181, Kluwer Academic Publishers, 1996.

G. S. Mamatha has completed her MTech from Visveswaraya technological University in the year 2004 in the field of Computer Science and Engineering. She is currently pursuing her Ph.D in Avinashi Lingam University for women; Coimbatore. She has 6 Years of academic experience in R.V.C.E. She is a member of ISTE. Her area of research includes Network security, Software Engineering and Multimedia systems

Dr. S. C. Sharma is Vice-Chancellor of Tumkur University, Tumkur, Karnataka. He pursued PhD in Mechanical Engineering from Mysore University, Doctor of Science in CSE from Kuvempu University, Doctor of Engineering from Avinashi Lingam University. The various positions he held includes as Adjunct Professor Of Engineering in West Virginia University, USA, Senior scientist, University of Wisconsin, Milwaukee, USA, State Government of Karnataka Nominee as Member of Executive Council, Member, Research Review Committee, Associate Editor, Research Journal Editorial Board, Syndicate member, Avinashi Lingam University, Coimbatore, Tamil nadu. His specialization areas include advanced materials, Metal Casting, Internet Enabled Automated System. He has got several Fellowships and awards for his contributions in academics and music field.