International Journal of Smart Sensor and Adhoc Network

Volume 1 | Issue 1 Article 7

July 2011

# An Algorithm to Detect Attacks in Mobile Ad Hoc Network

Radhika i Sain
*Computer Science Department, Ambedkar Institute of Technology, New Delhi, India*, myself_radhika@yahoo.co.in

Manju Khari
*Computer Science Department, Ambedkar Institute of Technology, New Delhi, India*, manjukhari@yahoo.co.in

## Recommended Citation

Sain, Radhika i and Khari, Manju (2011) "An Algorithm to Detect Attacks in Mobile Ad Hoc Network," *International Journal of Smart Sensor and Adhoc Network*: Vol. 1 : Iss. 1 , Article 7.
DOI: 10.47893/IJSSAN.2011.1006
Available at: https://www.interscience.in/ijssan/vol1/iss1/7

# An Algorithm to Detect Attacks in Mobile Ad Hoc Network

**Radhika Saini[1], Manju Khari[2]**
*Computer Science Department, Ambedkar Institute of Technology, New Delhi, India*
*Email Id: myself_radhika@yahoo.co.in[1], manjukhari@yahoo.co.in[2]*

***Abstract— Each node in Mobile Ad Hoc Network (MANETs) communicates with each other for transferring the packet (or data) to destination node. Any anomalous behavior of a node can confine it from executing this operation and even can disturb the whole network process. Therefore, the need of monitoring the nodes arises to keep a check on the behavior of a node. In this paper, an algorithm is proposed to monitor the nodes & to check if a node is any under attack or not. Moreover, a second layer of security is added which is furnished by a testbed to monitor the nodes.***

***Keywords- Mobile Ad Hoc Networks (MANETs), Nodes, Availability, Security, Attacks.***

## I. INTRODUCTION

Mobile Ad Hoc Network is a kind of network which does not require any fixed infrastructure (or central entity) to work. Such network can be formed within few minutes which consist of mobile nodes. An example of MANETs is bluetooth [1] where data is transferred between mobile nodes like cellular phones or laptops. In MANETs, each node works as a host as well as a router i.e. a node can transmit and receive the packets as a host and routes the packet to the destination as a router. Each node, before forwarding the packet to next node, decides the routing protocol [2] to route the packet.

A packet can reach the destination node within a single-hop or in multi-hop.

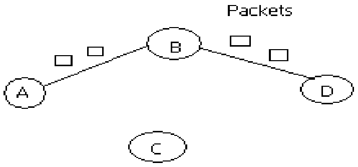


Figure 1-Packet forwarding in Hops

For example in figure 1, A is the source and if destination is node B then packet reaches in single-hop and if destination is node C then packet reaches through multiple hops. All the links between nodes are wireless. Military, emergency operations (like crowd control, search & rescue, commands operations) and collaborative computing are the fields where mobile ad hoc networks can be utilized.

MANETs has numerous security issues [3][4] like open wireless medium, shared radio broadcast channel, limited bandwidth, resource constraint and dynamic network topology which makes such network vulnerable to attacks [5] (eg. Blackhole attack, Wormhole attack, Rushing attack etc). These issues are exploited by intruder which breaches the security principles [6] (Confidentiality, Integrity, Availability, Authentication, Non-Repudiation) .Therefore it is mandatory to preserve all the security principles so that the entire network operation should not get disturbed. This paper is organized as follows: Section II presents the related work on proposed methods for detecting nodes under attacks. Section III describes the design of algorithm proposed in this paper. In section IV, an algorithm is proposed which will detect the whether a node is under classified attack or unclassified attack or not under any attack. Conclusion and future work is given in Section

## II. RELATED WORK

Every node in MANETs can take part in network operations if it is not under any attack. Any compromised node in the network can disturb the whole process. Therefore it is important to keep a check on the behavior of a node to ensure that it is not under any attack. Numerous methods have been proposed to detect the status of nodes which are as follows:

- Intrusion Detection Systems (IDS) – Anomaly based IDS is mainly used in MANETs to detect any kind of intrusion in the network. Profiles are maintained in databases of IDS to match the anomaly. These profiles can be static or dynamic in nature. The problem with such system is that it is difficult to make a perfect profile. Moreover false alarm rate is higher [7].

- Random Walker Detectors (RWD) – This detector moves randomly from one node to other node to detect the node’s activities. It monitors each node for a malicious behavior and migrates to the selected node. This RWD has a specification based detection engine for comparing the behavior of nodes [8].

- Watchdog – This method proposed the concept of a watchdog node which has high power and high transmission range than other ordinary nodes. This node watches and monitors the surrounding nodes. It keeps the node's data in its buffer and compares it after a new node receives it. Watchdog node is also called path rather [9].

- A method was proposed to detect the malicious nodes in the network by calculating the routes mainly the shortest route and re-routes the packet around them. This approach withstands the attacks in mobile ad hoc networks and based on routing protocols [10].

- Another method based on watchdog was introduced which was based on AODV (Ad-hoc On-demand Distance Vector) routing protocol. A credence based mechanism determines a node's credit standing [11].

- Security framework proposed for availability in which every node is monitoring its nearest neighboring nodes. The monitoring results are cross-validated after packet forwarding process. In this approach, each node has a valid certificate which indicates that this node is not under any attack [12].

- A model was proposed to check the status of a node in which an anomaly based IDS monitors the node in the network. When an anomaly is found, it simply checks its database classification for a match. If the anomaly matches then the attack handled otherwise it considered as a negligible anomaly [13]. This negligible anomaly can be an attack which is not defined in the classification. Such attacks are known as unclassified attacks which a classification fails to detect. Moreover this model can stuck in the loop of negligible anomaly in case of unclassified attack. Therefore it fails to detect such attacks. This model has a single layer of security which is furnished by anomaly based IDS.

The motive of this paper is to provide a second layer of security to the state model proposed in [13]. This second layer security is furnished through a testbed which will simulate the negligible anomaly. After simulation, it will give result based on it. Result can be an attack or a negligible anomaly.

## III. Design of Proposed Algorithm

Proposed algorithm design mainly has four parts- Anomaly based Intrusion Detection System (IDS) [7][13], a classification [13], a testbed [14][15] and a defense [13]. Anomaly based IDS monitors the node's activity constantly. If any anomaly (deviation) from normal behavior is found in the network then IDS uses it own database ( i.e. the classification) to match the abnormal behavior. Matching is done with the help of a classification. If it is matched then that particular node is under attack and is not available for further use. And if is not matched then the testbed simulates the behavior to test whether that can an unclassified attack which classification fails to match or a negligible anomaly. The unclassified attack can be a known or unknown attack.

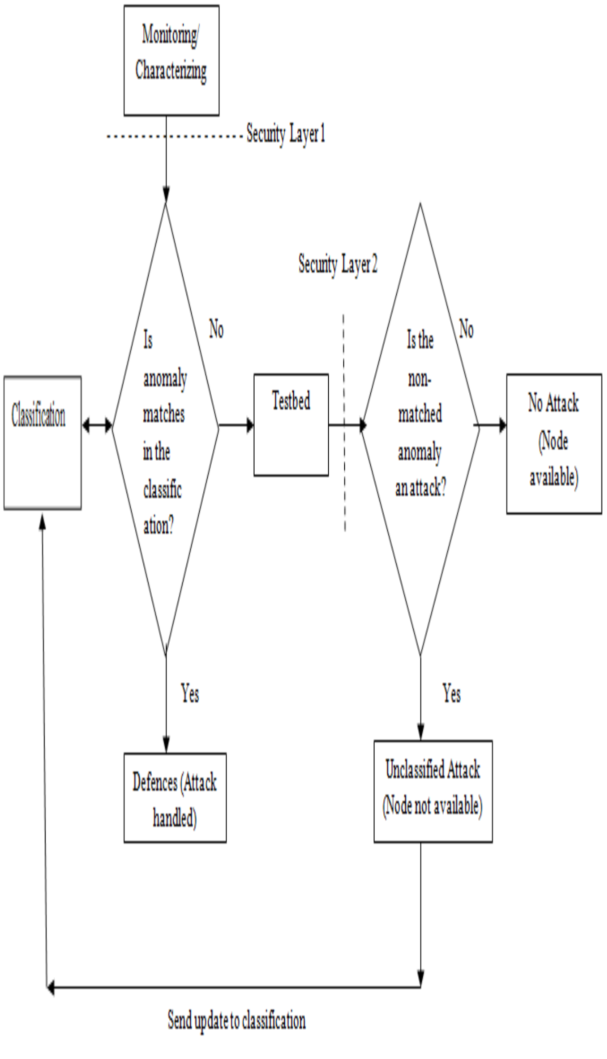
Proposed algorithm is an advanced version of the state model proposed by Bharat Bhargava, Ruy de Oliveira1,Yu Zhang and Nwokedi C. Idika [13] in which a classification matches the anomaly with its stored abnormal behavior and if it is not matched then it is returned as a negligible anomaly. This negligible anomaly can be an unclassified attack. To find such unclassified attack, this algorithm is proposed.

## IV. Proposed Algorithm

Definition of Unclassified attacks – These are the attacks which a classification fails to detect. Such attack can be an already known or a new attack. And that is why called the unclassified attacks.

In Ad Hoc Network, number of attacks [5] is defined through which an intruder attacks. An intruder always tries to find new and different ways to attack the network so that he cannot easily get caught. Therefore, there is a need of such a method which can easily detect the defined attacks as well as the other attacks. In this section, such an algorithm is proposed which provided two layer of security to the ad hoc networks – through IDS and then testbed. IDS will monitor nodes for any anomaly and testbed will simulate the unmatched anomaly.

Description of Algorithm – In proposed algorithm given below, each node is monitored with the help of anomaly based IDS. IDS already contain the abnormal (malicious) behavior of a node in its database (present in classification). If any anomaly is detected by the IDS then the classification matches the malicious activity of a node with the stored activities in the database. If it matches then the attack is handled through the defined defences and if it does not match then the testbed simulates that particular behavior of a node and determines whether that activity is an unclassified attack which can be a known or unknown attack or it is negligible anomaly which is a normal behavior. The input to the testbed is the output from the classification in case of non-matched anomaly. Then this update is send to the IDS database. If a node is under any unclassified attack then that node will be considered unavailable for use and if a negligible anomaly is found then it is available for services to provide.


Monitoring/ Characterizing
Security Layer 1
Security Layer 2
Is anomaly matches in the classific ation?
No
Classification
Testbed
Is the non-matched anomaly an attack?
No
No Attack (Node available)
Yes
Yes
Defences (Attack handled)
Unclassified Attack (Node not available)
Send update to classification

Proposed Algorithm

## V. Conclusion and Future Work

The algorithm proposed in this paper will be able to detect all the classified and unclassified attacks in mobile ad hoc network. Unclassified attack can be an already existing attack which is known or can be a new attack (or unknown attack). The update mechanism to the IDS makes the data up-to-date which helps in finding the attack more easily. This algorithm will decrease the false alarm rate due to use of a testbed. Testbed will always simulate the non-matched behaviors to find the attacks and prevent the network from intruders.

Now the implementation of both the proposed work can be done on any simulator like NS2 or matlab and their results can be compared to know their respective efficiency. Designing a suitable testbed is a crucial task to do. Moreover time taken by both the methods and accuracy in detecting the attacks can be measured. Defining and setting the anomalous (or malicious) behavior of a node is difficult.

## References

*[1] C.Siva Ram Murthy and B S Manoj, —Mobile Ad Hoc Networks - Architecture and Protocols, Pearson Education, ISBN 81-317-0688-5 ,2004*

*[2] Charles E. Perkin —Ad Hoc Networking, Pearson Education, ISBN 9780201309768, January, 2001*

*[3] Sheikhl, R Chandee, M. and Mishra, D. -Security Issues in MANET: A Review, IEEE 2010*

*[4] Rai, Pradeep and Singh, Subhha , —A Review of MANETs Security Aspects and Challenges , IJCA Special Issue on Mobile Ad Hoc Networks, 2010*

*[5] B. Wu et al, —A Survey of Attacks and Preventions in Mobile Ad Hoc Networks, Wireless/Mobile Network Security, Springer, Vol 17, 2006.*

*[6] Jangra1,A. Goel,N. Priyanka and Bhati,K. - Security Aspects in Mobile Ad Hoc Networks (MANETs): A Big Picture, International Journal of Electronics Engineering, pp. 189-196, 2010*

*[7] Sahu, S and Shandilya, S K - A Comprehensive Survey On Intrusion Detection In Manet, International Journal of Information Technology and Knowledge Management, Volume 2, No. 2, pp. 305-310 July- December 2010*

*[8] Panos,C Xenakis,C and Stavrakakis,I - A Novel Intrusion Detection System for MANETs International Conference on Security and Cryptography (SECRYPT) 2009*

*[9] Patcha,A and Mishra,A - Collaborative Security Architecture for Black Hole Attack Prevention in Mobile Ad Hoc Networks, IEEE. 2003*

*[10] Mamatha,G. and Dr. Sharma,S. – A Highly Secured Approach against Attacks in MANETS, International Journal of Computer Theory and Engineering Vol. 2 No. 5 1793-8201, October 2010*

*[11] Jinghua,L. Peng,G. Yingqiang,Q. and Gui,F. – A Secure Routing Mechanism in AODV for Ad Hoc Networks, IEEE 2007*

*[12] Jaisankar,N. and Swamy,K D – A Novel Security Framework for Protecting Network Layer Operations in MANETs, International Journal of Engineering and Technology Vol. 1, No. 5, December 2009*

*[13] Bhargava,B Oliveira1,R Zhang,Y and Idika, N - Addressing Collaborative Attacks and Defense in Ad Hoc Wireless Networks, IEEE International Conference on Distributed Computing ystems Workshops, 2009*

*[14] Barolli,L. Ikeda,M. Xhafa,F. and Duresi,A. – A testbed for MANETs: Implementation, Experiences and Learned Lessons, IEEE 2010*

*[15] Li,L. and Zhang,H. – Research on Designing and Implementing an Experimental MANET Testbed, IEEE International Conference on Communication Software and networks, 2009*