Journal of Information and Operations Management
ISSN: 0976–7754 & E-ISSN: 0976–7762 , Volume 3, Issue 1, 2012, pp-210-212
Available online at http://www.bioinfo.in/contents.php?id=55

MALICIOUS NODES DETECTION IN MOBILE AD HOC NETWORKS

SHOBHA ARYA[1] AND CHANDRAKALA ARYA[2]

[1]Computer Science & Engineering, G.B. Pant Engineering College, Pauri, India
[2]Computer Science, Pal College of Technology & Management, Haldwani, India
*Corresponding Author: Email- arya.chandrakala@gmail.com,01shobha@gmail.com

Received: December 12, 2011; Accepted: January 15, 2012

Abstract- The issue of security is a critical problem when implementing mobile ad hoc networks (MANETs) is widely acknowledged. One of the different kinds of misbehavior a node may exhibit is selfishness. A selfish or indiscipline node wants to preserve own resources while using the services of others and consuming their resources. Malicious nodes that disobey the standard, degrades the performance of well-behaved nodes significantly. One way of preventing selfishness in a MANET is a detection and exclusion mechanism. In this paper, we describe different method for detecting indiscipline or malicious nodes in mobile ad hoc network.

Keywords- MANETs, Ad Hoc, Security, Robust, Malicious nodes etc.

Citation: Shobha Arya and Chandrakala Arya (2012) Malicious Nodes Detection in Mobile Ad Hoc Networks. Journal of Information and Operations Management ISSN: 0976–7754 & E-ISSN: 0976–7762, Volume 3, Issue 1, pp-210-212.

Introduction

The MANET is the collection of mobile users that communicate over relatively bandwidth constrained wireless links. Since the nodes are mobile, the network topology may change rapidly and unpredictable over time. It is also known as infrastructure less network. MANETs can form stand-alone groups of wireless terminals, but some of these may be connected to some fixed network.

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. 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. MANETs is able to configure themselves on-the-fly without intervention of a centralized administration. The terminals in the ad hoc network can not only act as end-system but also as an intermediate system (routers). It is possible for two nodes which are not in the communication range of each other, but still can send and receive data from each other with the help of intermediate nodes which can act as routers. This functionality gives another name to ad hoc network as “multi-hop wireless network”.

There are different routing attacks which appear in network layer during wireless transmission of messages. These attacks are caused by either some internal or external intruders. To accomplish our goal, we have done literature survey in gathering information related to various types of attacks and solutions. We have observed that secure routing protocol is the essential requirement and there is no general algorithm that suits well against the most commonly known attacks. In our paper we propose an approach that deals with the network layer attacks.

Related Work

In MANET a lots of research have been done in malicious node detection like A Review of Current Routing Attacks in Mobile Ad hoc Networks [1], Security in Ad hoc Networks [2], Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications [3], A Robust Approach to Detect and Prevent Network Layer Attacks in MANETS [4], Behavior Based Anomaly Detection

Technique to Mitigate the Routing Misbehavior in MANET [5]. The current research is based on network layer attack and network layer security for delivery of packets. The routing message exchange within the packets between nodes is consistent with the protocol specification. The protocols can be classified as: secure ad hoc routing protocols and secure packet forwarding protocols. The paper mainly discusses about the network-layer security.

Proposed Approach

There are different routing attacks which appear in network layer during wireless transmission of messages. These attacks are caused by either some internal or external malicious intruders. The routing attacks are black hole, worm hole, rushing attack etc. become robust in network layer. When the malicious node pretend itself a valid route to the destination and join the routing correctly but later goes on ignoring all the packets that pass through it rather than forwarding them. This attack is known as Black hole attack. While when the nodes forward some selective packets to the destination node instead of all. Then this type of attack is called grey hole attack. To resolve these types of problems we ensure that each node in a network forwards packets to its destination properly.

In the security to network layer in MANETS we propose here a new secure approach which uses a simple acknowledgement approach, principle of flow conservation and encryption. Here we use DSR protocol to detect malicious node and provide secure method against routing attacks.

In our approach we detect the malicious nodes while computing the route in the network and re-routing the packets around it, find the shortest path among them. These protocols are basically existing ad hoc routing protocols like AODV, DSDV and DSR, designed to handle attacks. The encryption is used while sending the packets from one node to another node. We use this approach to ensure the security to network layer in MANETs against attacks.

The design of our proposed algorithm provides security from more than two attacks. In our algorithm we used encryption, acknowledgement and principle of flow conservation approach to security against attacks.

Before discussing algorithm some basic terms are given for algorithm development:

- **Start Time**- The packet sending time by the source node.
- **End Time-**The time taken for the acknowledgement to reach back the source**.**
- **Round Trip Time (RTT)-**The total time taken for transmission.
- To count the number of packets sent by counter **Cpkt** is used.
- To count the number of lost packets counter **Cmiss** is used.
- According to principle of flow conservation the limit of tolerance is set to some threshold value i.e. in this algorithm it will be 20%.
- When an acknowledgement received by the sender exceeds the RTT time limit, then the data packet will be accounted as a lost packet. The RTT time limit is set to 20 milliseconds.

We calculate the (Cmiss/Cpkt) ratio. If the calculated ratio is greater than the limit of tolerance threshold value 20%, then the link is said to be misbehaving otherwise properly behaving. Parallelly using the ratio value, the corresponding attacks will be identified.

In our algorithm encryption method is applied on message from sender side and the message is decrypted at receiver side. In data format only 48 bytes are sent at a time. So the message is longer than 48 bytes is divided into packets of 48 bytes each. Each time when a packet is sent the counter Cpkt gets incremented and the time will be the start time.

- At the receiver node the message is decrypted and an acknowledgement ACK packet is sent back to the sender through the intermediate nodes. Else when the decrypted message doesn't match then the acknowledgement packet sent back to the sender through the intermediate node consists of "CONFIDENTIALITY LOST".
- At Sender side, when acknowledgement reached, it computes the time taken for this acknowledgement to reach (end time). These steps are perform by the sender side-

```
    a. IF
   Total Transmission Time taken (end-start) > pre-specified
    interval( 20 ms).
  Then
    Rejects the corresponding data packet, announce it as lost
     data packet and Increment
    the Cmiss counter.
    b. Else
    It checks for the contents of acknowledgement field.
      If
        The ratio of (Cmiss/Cpkt)>=20%
      Then
```

i) The intermediate node is malicious and a new field "CONFIDENTIALITY LOST" is built in to the acknowledgement frame.

ii) Sender switches to an alternate intermediate node for the future sessions. Otherwise another new field "ACK" is built in to the acknowledgement frame.

iii) This intermediate node is considered to be behaving as expected and transmission is continued with the same intermediate node. Such intermediate nodes can be called genuine nodes.

The algorithm mainly identifies four attacks parallelly namely packet eavesdropping, message tampering, black hole attack and gray hole attack.

- **Packet eavesdropping**: In Packet eavesdropping while delivery of packets some of the malicious nodes tend to drop packets intentionally to save their own resources and disturb the network operation. It can be determined by the value of the (Cmiss/Cpkt) ratio.
  (i) If (Cmiss/Cpkt)>20%,
  (ii) Then link contains a malicious node launching packet eavesdropping attack.
- **Message tampering:** Sometimes network security integrity principle is not followed by the intermediate nodes. They will tend to tamper the data that has been sent either by deleting some bytes or by adding few bytes to it. This is an intentional malicious activity by the intermediate malicious nodes.

(i) If the acknowledgement frame sent by the receiver contains "CONFIDENTIALITY LOST" field in it. Then the node is called tampered the data sent.

(ii) If Ratio (Cmiss/Cpkt)>20%, Then link is called misbehaving and attack is message tampering.

- **Black hole attack:** If the ratio (Cmiss/Cpkt)>=1.0, Then all the sent packets are said to be lost or eavesdropped by the malicious node.
- **Gray hole attack:** When the nodes forward some selective packets to the destination node instead of all. Then this type of attack is called grey hole attack. In this attack malicious intermediate nodes selectively eavesdrop the packets i.e. 50% of the packets, instead of forwarding all.

Thus
If the ratio (Cmiss/Cpkt)>0.2 and (Cmiss/Cpkt) = 0.5,
Then half of the packets that have been sent are eaves dropped by the malicious node.

Conclusion

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.

References

[1] Khokhar Rashid Hafeez, Ngadi Md Asri and Mandala Satria (2008) *International Journal of Computer Science and Security* 2(3):18-29.

[2] Bingwen He, Hägglund Joakim and GuQing (2005) *“Security in Adhoc Networks”, An essay produced for the course Secure Computer Systems* HT2005 (1DT658)

[3] IEEE Std. 802.11 (1997) *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*.

[4] Mamatha G.S., Sharma S.C. (2009) *International Journal of Computer Science and Security,* Vol (4): Issue (3).

[5] Sundararajan TVP., Shanmugam A. *International Journal of Computer Science and Security,* Vol (3): Issue (2).

[6] Zawtun and Maw Aung Htein (2008) *World Academy of Science, Engineering and Technology,* 46.

[7] Dhanalakshmi S., Rajaram M. (2008) *International Journal of Computer Science and Network Security,* vol-8 No.10.

[8] Oscar F. Gonzalez, God win Ansa, Michael Howarth and George Pavlou (2008) *Journal of Internet Engineering*.

[9] Moumita Deb (2008) *World Congress on Engineering and Computer Science*.

[10] Xiaoxin Wu, David K.Y. (2007) 3*rd International conference on secure Communications*, pp. 310-319.

[11] Murali Kodialam, Lakshman T.V. (2003) *IEEE INFOCOM*.

[12] Sun choi, Doo-young Kim, Do-hyeon Lee, Jae-il Jung, *International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing,* pp.343-348 .

[13] Song N., Qian L. and Li X. (2005) 19*th IEEE International Parallel and Distributed Processing Symposium*.