Survey on Encroachment Sensing Scheme over the MANET

Apurba Shukla
Dept. of Information Technology
VIT, Mumbai, India
apurvashukla1991@gmail.com

Prof. Sachin Deshpande
Dept. of Computer Engineering
VIT, Mumbai, India
sachin.deshpande@vit.edu.in

Abstract— MANET (Mobile ad hoc network) is a collection of mobile nodes which dynamically self-organizes in erratic and transitory network topologies. Nodes in MANET can move autonomously in any direction and continuously changing the topology over the period. Each single node works evenly as a source and a recipient. MANET are more inclined towards security issues due to open medium and wide distribution of mobile nodes. It is vital to construct effective intrusion detection processes to preserve MANET from attacks. This paper introduces the various IDS schemes over MANETs, their pros and cons. This paper will be valuable to classify the suitable IDS scheme for a particular attack.

Keywords - *Mobile Ad hoc networks, Intrusion Detection System (IDS), topology, AD HOC Networks.*

*****

I. Introduction

In MANET, a set of nodes that are interacting with each other may represent the possibility for personal communications and interaction among mobile users to implement the routing in order to enable the communication by using dynamic paths. These cluster of motile nodes have both connectionless data transmitter and the receiver. One of the main asset of MANET is it allows data to communicate between different parties and still maintain their mobility. In emergency conditions, a fixed infrastructure will not be convenient or it may not be viable enough to install a new one, like natural calamities, human induced disasters, military or medical cases. It is in such situations that the quick deployment and minimal configuration features of MANETs come as an advantage. Due to these reasons, they are largely used in the industry recently. But these features itself acts as disadvantages to the MANET applications. Absence of centralized system and management, causes MANETs vulnerable to the attackers. MANET is highly vulnerable to different type of attack due to its characteristics [2]. As the expansion in wireless devices, trust is introduce to measure the trustworthiness of node to participate in any expected operation. However security mechanism involving trusted third parties may no longer be viable in mobile ad hoc networks [4]. So development of more reliable security mechanism is required.

An intrusion detection system (IDS) specifically designed for MANETs are needed since MANETs do not have a centralized management system. Intrusion detection (ID) in MANET is a lot more complex than in normal wireless networks that are fixed because it is difficult to collect the required data from the MANETs. Also, difficulty arises due to the intrinsic characteristics of MANETs that are mentioned before. Although many mechanisms and routing protocols are introduced each of them has one or more vulnerabilities. Research on MANET and implementation has become a vital task to be done. When a malicious node is found the node has to be either repaired or another route has to be established. In most of the persisting techniques the nodes when found slightly malicious is completely isolated from the network which will make splitting of the network and thereby causing communication problems between the nodes.

II. Key Concepts

A Misbehavior Detection in Manet

The primary challenge in MANET is to detect misbehavior and mitigate same. There are disparate schemes proposed to avoid nodes misbehavior in MANET which can be classified as:

- Credit Based Schemes

In this scheme, credit/incentives are provided to the nodes performing network operations. Extensively proclaimed credit based schemes are Packet Purse Model (PPM) and Packet Trade Model (PTM). These schemes may need extra protection for payment system.

- Reputation Based Schemes

In this scheme, nodes collectively co-operatively detect and declare misbehavior of nodes in the network. Such a notification is carried out throughout the network and misbehaving node is removed from the network. ‘Watchdog & Pathrater’ and ‘Confidant Protocol’ are examples of reputation based scheme.

- Acknowledgement Schemes

In this scheme, acknowledgements are sent by the receiver to sender about the successful reception of data packets. There are varied acknowledgement based schemes proposed for misbehavior detection such as EAACK, TWO-ACK, AACK etc. Acknowledgement schemes proposed have been discussed.

B. Intrusion Detection System

IDSs usually act as the second layer in MANETs. Intrusion defined as a set of actions that attempt to compromise the integrity, confidentiality and availability of a resource [1] and an intrusion detection system is a system for the detection of such iterations. IDS consists the following components: data collection, detection and response. The first component data collection is responsible for collection and pre-processing and transferring data to common format [3]. IDS uses input from various data source such as system logs, network packets, etc. The second component detection is used to analyses the data and to detect intrusion attempts and the detected intrusions are sent to the response component. There are many intrusion detection schemes used. When an intrusion is detected, a suitable response is triggered depending on the response policy. Responses can be passive or active to detected intrusions. Passive responses just raise alarms and inform the proper authority. Active responses seek to mitigate effects of intrusions.

III. Literature Survey

A large number of IDS techniques are proposed to ensure secure communication of data packets in the network.

- The Watchdog scheme proposed by Marti, Giuli, and Baker, consists of two portion namely watchdog and path rater. A watchdog identifies the misbehaving nodes by eavesdropping on the transmission of the next hop. A path rater then helps by combining knowledge of misbehaving nodes and routing protocols to avoid the reported nodes in future transmission. In Watchdog [6], recently sent packets are kept in a buffer and overheard packets are compared with those in the buffer. If it matches, the packet in the buffer is removed. If the packet prevails in the buffer for a long time, a failure tally is increased for that node which was supposed to forward the packet. A threshold is set, overreaching which the node is considered misbehaving and the source node is notified about that node. Watchdog works properly only if it has the knowledge about where the packet would be in two hops.
  Drawback : Detecting misbehavior in the presence of ambiguous collisions, receiver collisions[7], limited transmission power, false misbehavior and partial dropping is problematic. In order to preserve its own battery resources some nodes purposely limit its transmission power.

- TWOACK is proposed by N. Nasser et al [9] is an acknowledgement based technique, to detect intrusion in MANET. TWOACK scheme is to weaken the influence of misbehaving node. The concept of this TWOACK is to send a two-hop acknowledgement to source node in the reverse direction but in same path. The TWOACK work is based on a dynamic source routing (DSR) is proposed by D. Johnson et al [5]. The working process is shown in figure 1. Node A forwards a packet to node B, node B forward the same packet to node C. Node C is two hops away from node A. Now node C direct TWOACK packet to node A. Then the node A will confirm the packet is transmitting to C by node B successfully. The TWOACK solve issues like receiver collision and limited transmission power, which is created in watchdog.

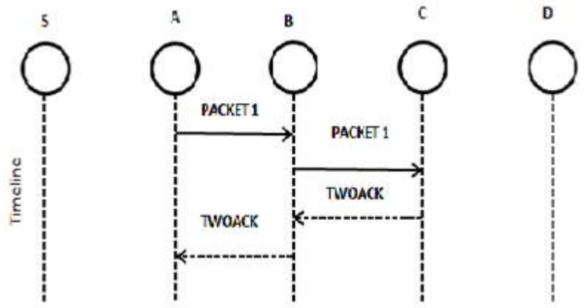

Figure 1: TWOACK scheme

Drawback : But problem associated with the TWOACK is due to frequent transmission TWOACK, it reduces battery power of nodes. So, it can decrease the life span of nodes in MANET. So it spoils the entire network. Considering the security, there is a need to guarantee that the acknowledgement packets are valid and authenticated.

.

- Sheltami et al [11] proposed AACK (Adaptive Acknowledgement Scheme) scheme. This is also an acknowledgement based network layer scheme and it is a combination of two existing schemes such as TWOACK and ACK. AACK scheme could reduce the network overhead but could not improve the network throughput. The figure 2 [12], below shows the ACK scheme.

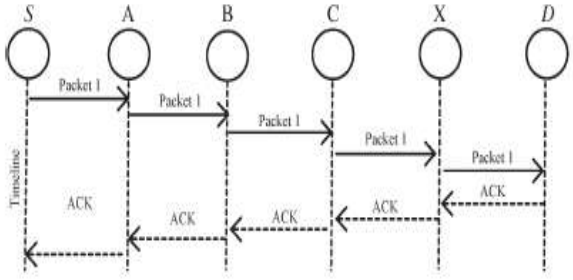

Figure 2: ACK (An End- End Acknowledgement)

It can be noticed that node S forwards the packet to the destination via the intermediate nodes such as A, B, C and X. The intermediate nodes forward this packet till the end node receives it. When the destination node receives this packet it in turn sends an acknowledgement packet via all the intermediate nodes down the line to the source in an opposite direction. If the ACK is not received within the predefined time period, then the data transmission between source and destination node is not successful, otherwise it is considered to be successful. If the data transfer is not successful, the source node switches from ACK mode to TWOACK mode by sending TWOACK packet. This way of adopting hybrid technique of combining both ACK and TWOACK scheme results in reduced network overhead.

Drawback : Fails to detect the malicious nodes in the presence of false misbehavior report.. Fails to detect the malicious nodes in the presence of forged acknowledgement packets.

- Michiardi and Molva [13] proposed a Collaborative Reputation (CORE) mechanism in which monitoring is done using a watchdog component. This is a passive acknowledgement based scheme. It stimulates the node cooperation by a collaborative monitoring proficiency and a reputation scheme. Each node computes reputation value for each of its neighbors using reputation mechanism which includes subjective reputation, indirect reputation and functional reputation. Based on the reputation values this technique detects the misbehaving nodes. CORE successfully prevents false allegations.
  Drawback : It cannot prevent colluding nodes from distributing false praises, which can gain misbehaving nodes' reputation.

- Packet Purse Model (PPM) addressed in [14] is a credit based scheme. In this scheme, the originator of the packet has to render for the packet forwarding function. The originator should have adequate amount of credits with it, for the packet to reach the end node. Each forwarding node will increment the number of beans with them by acquiring one or more beans from packet. Drawback : This scheme has flaw that it is difficult to estimate the number of beans required to reach a given destination.

- In the Packet Trade Model (PTM) in [14] each node is having beans initially. Here a packet does not take beans along with it, but it is traded for beans via intermediate nodes. Each intermediate node attempt to sell the packets for more beans. In this scheme, each intermediary buy the packet from previous node for some beans and sell those packets to the next intermediate nodes for more number of beans. The advantage of this scheme is that the originator does not have to know the number of beans required to send the packets in advance.

  Drawback : It requires extra protection for payment system.

- CONFIDANT (Cooperation Of Nodes, Fairness In Dynamic Ad hoc NeT-works) scheme proposed by Buchegger and Le Boudec [8] is a reputation-based scheme. It is made up of four components. These components observe their neighbor nodes, rate them, rate the path and also send and receive the alarm messages. The four components of CONFIDANT protocol are:
  The Monitor: Every node in the network continuously monitors the behavior of the node next to it. If any suspicious event is detected, the details of such event are passed to the next component i.e. Reputation System.

  The Reputation System: The rating of the suspected node is modified (either incremented or decremented) based on the details such as frequency of the suspicious event and also significance of such event.

  The Path Manager: When the node rating crosses the predefined threshold the control is passed to this component by the Reputation System. This system then controls the route cache.

  The Trust Manager: This component propagates the alarm message to all the nodes in the network.

  Drawback : The monitor component in this scheme works same as that of the watchdog scheme in which it observes and overhears the next node's transmission. Hence this scheme also has the same limitations as that faced by the watchdog scheme.

- EAACK (Enhanced Adaptive Acknowledgement) technique employed by Elhadi et al alleviates three weaknesses of Watchdog viz. False misbehavior, limited transmission power and receiver collision [12]. EAACK consists of 3 parts: acknowledgement ACK, Secure Acknowledgement S-ACK and Misbehavior Report Authentication MRA. This scheme is capable of detecting malignant nodes even in case of false misbehavior report. The difference from the previous work lies in the fact that the source node has to turn on the MRA mode and confirm the misbehavior rather than believing blindly that misbehavior occurred [12]. Alternate route is used by initiating a new route discovery confirm misbehaving report. If the destination obtain MRA packet, it is concluded that the report is false and whoever has generated that report is marked as malicious else it is concluded that the misbehavior report is trusted. In order to assure the integrity, all the acknowledgement packets in this scheme are digitally signed by nodes.
  Drawback : The RSA scheme utilises more battery power and suffers from the extra amount of network overhead.

IV. CONCLUSION

The rapid mobility and geographically scattered nature of MANETs is exposed to attacks, esp., network layer attacks. This paper, have analyzed some of the significant existing misbehavior or intrusion detection mechanisms. The detection methods also have to be protected. Ad hoc networks have been a vital section of research with lots of practical applications. The Reputation based schemes mostly based on overhearing technique have many drawbacks and led the way to active acknowledgement based schemes. The credit based schemes requires the source node to keep the amount of virtual money required for the transaction of the packet. These schemes impose a load on the source node. Acknowledgement based schemes discussed in this paper detects and prevents the misbehavior in the MANET. IDS can be viewed as a defender that automatically detects malicious activities within a host or network. As security is greatest issue in MANET, this paper can act as a source for the masses working towards MANET. Each of the above surveyed methods demonstrates and shows better in some extent and not in entire categories. Prevention alone is not the sufficient for this; hence Intrusion Detection Systems have come into focus. Various existing IDS were discussed in this paper. Every IDS has its own limitations. Even though highly effective detection mechanisms have been proposed, invaders often use new methods to attack the networks. Due to that, elaborating new techniques for intrusion detection based on the newly emerging attacks is a very important area of research. Thus this is a never ending research area.

References

[1] Heady R, Luger G, Maccabe A, Servilla M (1990) "The architecture of a net-work level intrusion detection system". Technical Report, Computer Science Department, University of New Mexico.

[2] Hadi Otrok, Joey Paquet, Mourad Debbabi and Prabir Bhattacharya, "Testing Intrusion Detection System In MANET: A Comprehensive Study", Fifth Annual Conference On Communication Networks and Services Research (CNSR'07), 0-76952835-X/07, IEEE Computer Society, 2007.

[3] Lundin E, Jonsson E. (2002) Survey of Intrusion Detection Research.Technical report 02-04, Dept. of Computer Engineering, Chalmers University of Technology

[4] Po-Wah Yau and Chris J Mitchell, "Security Vulnerabilities in Ad Hoc Networks", the work reported in this paper formed part of networks and services area core 2 research program of the virtual center of excellence in mobile and personal communications, mobile VCE, 2004.

[5] D. Johnson and D. Maltz, "Dynamic Source Routing in ad hoc wireless networks," Mobile Computing. Norwell, MA: Kluwer, 1996, ch. 5, pp. 153–181.

[6] S. Marti, T.J. Giuli, K.Lai and M. Baker, "Mitigating Routing Misbehaviour in Mobile Ad Hoc Networks",(2000), Proceedings of International Conference on Mobile Computing and Networking, pp 255- 265.

[7] J. Jubin and J. Tornow. The DARPA Packet Radio Network Protocols. In Proceedings of the IEEE, 75(1):21-32, 1987.

[8] S. Buchegger and J.-Y. Le Boudec, ―Performance Analysis of the CONFIDANT Protocol: Cooperation of Nodes, Fairness in Dynamic Ad-Hoc Networks,*Proc. MobiHoc*, June 2002.

[9] N. Nasser, "Enhanced Intrusion Detection Systems for Discovering Malicious Nodes in Mobile Ad Hoc Network", 2007.

[10] S.N.Chobe, "An Acknowledgement Based Approach for Routing Misbehavior Detection in MANET with AOMDV". International Conference on Mobile Computing and Networking, pp 255- 265.

[11] T. Sheltami, A. Al-Roubaiey, E. Shakshuki, and A. Mahmoud, "Video transmission enhancement in presence of misbehaving nodes in MANETs," Int. J.Multimedia Syst., vol. 15, no. 5, pp. 273–282, Oct.2009.

[12] Elhadi M. Shakshuki, Senior Member, IEEE, Nan Kang, and Tarek R. Sheltami, Member, IEEE,EAACK—A Secure Intrusion-Detection System for MANETs IEEE TRANSACTIONS ON INDUSTRIAL ELECTRONICS, VOL. 60, NO. 3, MARCH 2013.

[13] P. Michiardi and R. Molva, "CORE: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks," in CMS'2002, Communication and Multimedia Security 2002 Conference, September 26-27, 2002.

[14] Buttyan, Hubaux, "Enforcing Service Availability in Mobile Ad-Hoc Networks", in Proc. ACM, pp. 8796, 2000.