A Practical Approach for Malicious Activity Detection in MANET

Nidhi Nigam
Department of Computer Science & Engineering
Acropolis Institute of Technology and Research, (M.P.), India

Abstract— In this Paper, wireless networks, security has been proposed which becomes the prime factor of concern. The mobility of the nodes, in these so called Mobile Ad hoc Networks (MANETS), furthermore leads to a situation where it is very difficult to establish secure data transmission. Since the use of mobile equipments such as cellular phones or laptops is tremendously increasing and because of limited physical security, vulnerability to attacks, including an attack known as the wormhole attack, has become a challenging work. The wormhole attack is very powerful and preventing the attack has proven to be very complex. A strategic placement of the wormhole can result in a significant breakdown in communication across a wireless network. This addresses the aforementioned gap by providing a proper definition and categorization of wormhole attacks against MANET by introducing a new cooperative, clock synchronized technique based on Reference Broadcast System (RBS), and discuss its effect on network performance. To improve network scalability and throughput, the concept of thread for each and every node of MANET is proposed. So that our proposed scheme has two phases namely, route discovery phase of AODV (Ad hoc on demand distance vector protocol) for routing, Principle of Hop count for threshold setting are combined to detect and isolate wormhole attacks in ad hoc networks. That manages how the nodes are going to behave and which to route the packets in secured way.

Keywords: Wormhole, AODV, Routing approaches, MANET, Reference Broadcast System (RBS)

I. INTRODUCTION

Nowadays, it is hard to imagine a world without the Internet. The World Wide Web has evolved into an entity intertwined with our lives. What started out as an academic/ military network meant to make the exchange of research information easier and then turned into a meeting place for people from all around the world, grew exponentially larger year by year till it became the platform for many commercial applications and services it is today [1]. For a long time though, we could only enjoy its advantages within the confines of our homes or offices. With the rapid development of mobile technologies however, the use of networks is not limited through earthbound cables anymore.

The potentials of such wireless networks are not fully explored yet. Mobile telephony is the most basic application making use of them, but the list only starts there. Combining peer-to-peer techniques with the opportunities that mobility offers, so called ad hoc networks have become an important field of research in recent yean ad hoc network is defined as "an autonomous system of routers (and associated hosts) connected by wireless links—the union of which forms an arbitrary graph. The routers are free to move randomly and organize themselves arbitrarily; thus, the network's wireless topology may change rapidly and unpredictably. Such a network may operate in a standalone fashion, or may be connected to the larger Internet operating as a hybrid fixed/ ad hoc network."[2].

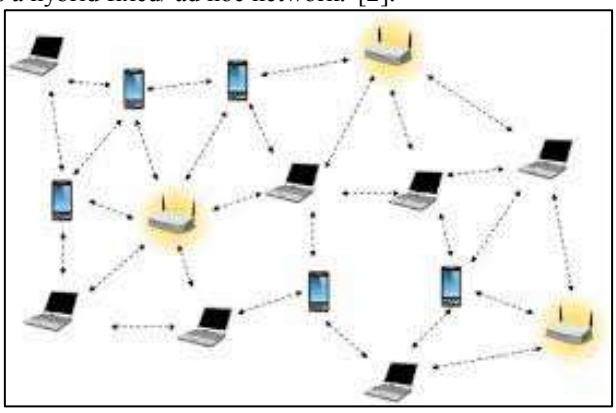

Fig. 1: A mobile ad-hoc network (MANET) consists of mobile hosts equipped with wireless communication devices

MANET properties[10] like insecure operational environment ,lack of infrastructure, lack of central controlling authority and others make them more vulnerable to attacks. A node may also misbehave because it is overloaded, broken, compromised or congested in addition, to intentionally being selfish or malicious. A malicious node drops packets or generates additional packets solely to disrupt the network performance and prevent other nodes from accessing any network services. Misbehavior can be divided into two categories: routing misbehavior (failure to behave in accordance with a routing protocol) and packet forwarding misbehavior (failure to correctly forward data Packets in accordance with a data transfer protocol).

The approach consists of an algorithm that performs two tasks:

1) Enables packet forwarding misbehavior detection and
2) Enables the prevention of nodes that are consistently detected to be exhibiting packet forwarding misbehavior [4].

A node that is detected for misbehavior is denied access to the network. The peers in the network will ignore any of such misbehaving nodes transmission attempts. Thus, misbehaving nodes are isolated from the rest of the network. The information regarding such node will be maintained by the source node, so that they should not take part in active communication. For security purpose, the source node uses a cryptography technique called hash code generation. This hash code will be appended in the data frame of sender node along with data [6]. Later, receiver node computes its hash code which is compared with the sender hash code for confidentiality check. Our criterion for judging malicious node detection is based on the estimated percentage of packets dropped, which is compared against a pre-established misbehavior threshold. Any node dropping packets in excess of this threshold is a misbehaving node, while those below the threshold are considered to be correctly behaving [5].

Attacks in Ad hoc networks are divided in to passive attacks and active attacks. This paper concentrates on active attacks considers the internal attacks like wormhole attack, gray hole attack, black hole attack, routing attacks, message tampering, sending data out of transmission range etc. Wireless cellular systems have been in use since 1980s. We have seen their evolutions to first, second and third generation's wireless systems. Wireless systems operate with the aid of a centralized supporting structure such as an access point. These access points assist the wireless users to keep connected with the wireless system, when they roam from one place to the other. The presence of a fixed supporting structure limits the adaptability of wireless systems. In other words, the technology cannot work effectively in places where there is no fixed infrastructure. Future generation wireless systems will require easy and quick deployment of wireless networks [6]. This quick network deployment is not possible with the existing structure of current wireless systems. Recent advancements such as Bluetooth introduced a new type of wireless systems known as mobile ad-hoc networks. Mobile ad-hoc networks or "short live" networks operate in the absence of fixed infrastructure.

They offer quick and easy network deployment in situations where it is not possible otherwise. Ad-hoc is a Latin word, which means "for this or for this only." Mobile ad-hoc network is an autonomous system of mobile nodes connected by wireless links; each node operates as an end system and a router for all other nodes in the network. Nodes in mobile ad-hoc network are free to move and organize themselves in an arbitrary fashion. Each user is free to roam about while communication with others. The path between each pair of the users may have multiple links and the radio between them can be heterogeneous. This allows an association of various links to be a part of thesamenetwork [7]. Amobilead-hocnet work is a collection of mobile nodes forming an ad-hocnetwork without the assistance of any centralized structures. These networks introduced a new art of network establishment and can be well suited for an environment where either the infrastructure is lost or where deploy an infrastructure is not very cost effective. As shown in Figure 2, an ad hoc network might consist of several home- computing devices, including laptops, cellular phones, and so on. Each node will be able to communicate directly with any other node that resides within its transmission range. For communicating with nodes that reside beyond this range, the node needs to use intermediate nodes to relay the messages hop by hop.

Routes are maintained by AODV as follows. If a source node moves, it is able to reinitiate the route discovery protocol to find a new route to the destination [8]. If a node along the route moves, its upstream neighbor notices the move and propagates a link failure notification message (an RREP packet with infinite metric) to each of its active upstream neighbors to inform them of the erasure of that part of the route. These nodes in turn propagate the link failure notification to their upstream neighbors, and soon until the source node is reached. The source node may then choose to reinitiate route discovery for that destination if a route is still desired. An additional aspect of the protocol is the use of hello packet.

II. A TYPICAL MOBILE AD HOC NETWORK

Mobile ad-hoc networks can operate in a standalone fashion or could possibly be connected to a larger network such as the Internet. Mobile ad-hoc networks can turn the dream of getting connected "anywhere and at any time" into reality. Applications of ad hoc network range from military operations and emergency disaster relief, to commercial uses such as community networking and interaction between attendees at a meeting or students during a lecture. Most of these applications demand a secure and reliable communication. Typical application examples include a disaster recovery or a military operation. Not bound to specific situations, these networks may equally show better performance in other places. As an example, we can imagine a group of people with laptops, in a business meeting at a place where no network services is present.

They can easily network the ir machines by forming an ad- hoc network [9]. This is one of the many examples where these networks may possibly be used. People have started using portable laptops to access Internet and other resources using wireless networks while moving. Another area which has generated a lot of interest recently, is wireless ad-hoc networks. An ad-hoc network is formed when two or more stations come together to form an independent network. Ad- hoc networks are also termed as infrastructure-less networks since as they do not require any prior infrastructure.

Two stations that are within transmission range of each other are called one hop neighbors. Multihop ad- hoc networks are ones in which the stations can talk to stations more than one hop away via intermediate stations. Cooperative ad-hoc networks are formed by several homogeneous wireless stations. All the stations cooperate with each other, i.e., the traffic for the stations that are more than one hop away is routed by the intermediate stations. The intermediate stations are called relaying stations. Cooperative multi hop Ad-hoc wireless networks consist of a group of stations connected to each other over one or more hops. If two communicating stations are more than one hop away, the intermediate stations route the packets from source to destination. Disaster management operations and battalion of soldiers are the example of applications of such cooperative ad-hoc wireless networks.

III. ROUTING APPROACHES IN MOBILE AD HOCNETWORK

Since the advent of Defense Advanced Research Projects Agency (DARPA) packet radio networks in the early 1970s, numerous routing protocols have been developed for ad hoc mobile networks. These are generally categorized as table-driven or proactive, on-demand or reactive and hybrid routing protocols. Table-driven or Proactive Protocols: Proactive routing protocols attempt to maintain consistent, up-to-date routing information between every pair of nodes in the network by propagating, proactively, route updates at fixed intervals.

As the resulting information is usually maintained in tables, the protocols are sometimes referred to as table-driven protocols. Representative proactive protocols include: Destination-Sequenced Distance-Vector (DSDV) routing, Clustered Gateway Switch Routing (CGSR), Wireless Routing Protocol (WRP), and Optimized Link State Routing

(OLSR). On-demand or Reactive Protocols: A different approach from table-driven routing is reactive or on-demand routing. These protocols depart from the legacy Internet approach. Reactive protocols, unlike table-driven ones, establish a route to a destination when there is a demand for it, usually initiated by the source node through discovery process within the network. Once a route has been established, it is maintained by the node until either the destination becomes in accessible or source.

IV. PROPOSED SCHEME

Wormhole attack in MANET is a passive attack and very hard to detect. None of the host is being compromised in this attack. Attacker just tunnel the packet and can analyses the network traffic. Our scheme work after the route establishment phase of AODV routing protocol. The protocol works in two phases one is route establishment and another is route maintenance. Between these phases actual communication takes place and here the proposed algorithm works.

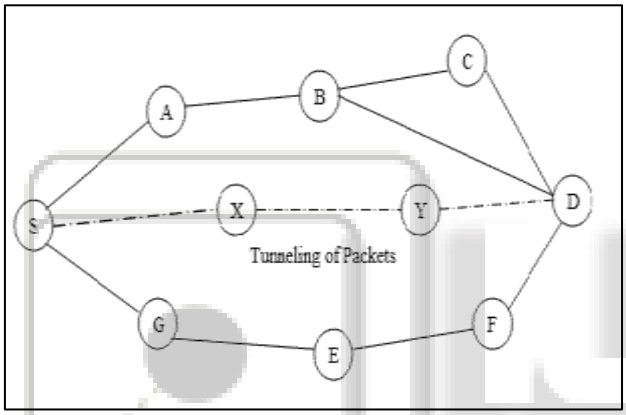

Fig. 2: Wormhole Attack

The above figure 3 shows MANET scenario which compromised by a pair of nodes (X, Y). There are several routes available between source S and destination D. AODV protocols forms the routing table with all available route between (S, D) pair. The set T consists of three routes, T = {S-A-B-D, S-A-B-C-D, S-G-E-F-D}.

A. Algorithm:

1) Initialize the network with AODV as routing protocol.
2) In route formation phase AODV creates a set of all available routes between a source destination pair.
3) Forms a routing table indicating the route and maximum hop count between a source destination pair.
4) After route setup, actual communication takes place and the hop count field of data packet is compared with the hop count of that route at random interval.
5) If the hop count differ the either route is changed or wormhole attack has occurred.
6) Now check the set of available routes, if the new route with same hop count exits then the network is not compromised otherwise attack has occurred.
7) The above algorithm helps to identify that the network has compromised and needs to recover.

V. ADVANTAGES OF THE PROPOSED SCHEME

AODV is a hop-by-hop routing protocol, which introduces a more dynamic strategy to discover and repair route when compared to DSR. Destination sequence numbers are used to avoid the problem of infinite loops. AODV maintains only active routes to reduce overheads and control traffic. This protocol is applicable for different levels of node density, mobility and loads. It is suitable for scenarios with moderate mobility and density networks. Efficient route establishment, resource reservations and less computational complexity since, the proposed approach uses a simple semantic security mechanism like hash code generation. This mechanism ensures more security since, other than receiver node nobody can compute hash code that is equal to sender's hash code. Monitors misbehaving nodes can be properly identified through the acknowledgement scheme.

Thus, problems such as ambiguous collisions, receiver collisions, and the ability of a node to control its transmission power do not exist in the approach.

VI. CONCLUSIONS AND FUTURE SCOPE

Wormhole attacks are significant problems that need to be addressed in wireless network security. Security of ad hoc networks has recently gained momentum in the research community. Due to the open nature of ad hoc networks and their inherent lack of infrastructure, security exposures can be an impediment to basic network operation. Security solutions for MANET have to cope with a challenging environment including scarce energy and computational resources and lack of persistent structure MANETS, this approach will tackle the issue in an efficient manner by reducing a number of attacks. The scheme discusses a semantic security mechanism to handle attacks based on packet dropping and message tampering, which can accurately detect the malicious nodes in the network. The malicious nodes identified are isolated for future sessions. In the proposed scheme, scope of enhancements and improvements are enormous. An immediate enhancement is evaluation of more network parameters. Further, the scheme can be made more secure against other types of possible network layer attacks that threaten the network. 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 scheme 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.

REFERENCES

[1] G.S. Mamatha, S.C. Sharma. "A New Secured Approach for MANETS against Network LayerAttacks".
[2] ShaliniJain, Dr. Satbir Jain, "Detection and prevention of wormhole attack in mobile adhoc networks",(2010).
[3] G.S. Mamatha, Dr. S.C. Sharma, "Network Layer Attacks and Defense Mechanisms in MANETS- A Survey",(2010).

[4] N.S. Raote, K.N. Hande,"Approaches towards Mitigating Wormhole Attack in Wireless Ad-hoc Network",(2011).
[5] KhinSandarWin,''Analysis of Detecting Wormhole Attacks in Wireless Networks",(2009).
[6] FaridNa¨ýt-Abdesselam, BrahimBensaou and TarikTaleb,"Detecting and Avoiding Wormhole Attacks in Wireless Ad Hoc Networks" (2007).
[7] Yih-Chun Hu, Adrian Perrig and David B. Johnson, "Packet Leashes: A Defense against Wormhole Attacks in Wireless Networks",(2002)
[8] Rouba ElKaissi,AymanKayssi, AliChehab andZaherDawy,"DAWWSEN: A Defense Mechanism Against Wormhole Attacks in Wireless Sensor Networks", (2005).
[9] ZakkiUlRehman Khan,Ms. Ankita Sharma,"Security Aspects of MANETs: A Review",International Journal of Computer Science and Mobile Computing, Vol.8 Issue.7, July- 2019, pg. 40-44.
[10] K Spurthi, T.N.Shankar, "A Research on Wormhole Attack in MobileAd-Hoc Networks",International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-8, Issue-1S4, June 2019

