ISSN No. 0976-5697

Volume 5, No. 8, Nov-Dec 2014

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

An Appraisal of Attacks in MANET and Fortification Methods

Prof.M.Anandhi
Department of Computer Science
Cauvery College for Women
Trichy, India

Prof.Dr.T.N.Ravi
Department of Computer Science
Periyar E.V.R College(Autonomous)
Trichy, India

Abstract: Mobile ad hoc networking is one of the most challenging areas of wireless networking. MANET consists of autonomous self-organizing mobile nodes. There is no centralized node or router in MANET where all network activity; including discovering the topology and delivering message must be executed by the nodes themselves. Network functions such as routing, address allocation, authentication and authorization must be designed to cope with a dynamic network topology. MANET is more vulnerable than wired network. Some of vulnerabilities in MANET are, Lack of centralized management, no predefined boundary, cooperativeness, limited power supply, mobility. Due to vulnerabilities, MANET facing lot of challenges and possibilities of security threats. This paper discusses the challenges, different types of attacks and various defense schemes.

Keywords: MANET, Attacks, Challenges, Security, Multilayer

I. INTRODUCTION

In early 1970s, the Mobile Ad hoc Network (MANET) was called packet radio network, which was sponsored by Defense Advanced Research Projects Agency (DARPA). In the 1990, the concept of commercial Ad hoc networks arrived with notebook computers and other viable communication equipments. An Ad hoc wireless mobile network is a collection of two or more devices equipped with wireless communications and networking capability. Ad hoc network is self-organizing and adaptive. Since ad hoc wireless devices can take different forms as shown in Figure 1, ad hoc nodes or devices should be able to detect the presence of other such devices as well as the type of devices and their attributes. There are no fixed radio base stations, no wires or fixed routers. Due to the presence of mobility, routing information will have to change to reflect changes in link connectivity.

In order to establish routes between nodes, which are farther than a single hop, specially configured routing protocols are engaged. The unique feature of these protocols is their ability to trace routes in spite of a dynamic topology. In the simplest scenarios, nodes may be able to communicate directly with each other, when they are within wireless transmission range of each other. However, Ad hoc networks must also support communication between nodes that are only indirectly connected by a series of wireless hops through other nodes.

MANET is more vulnerable than wired network due to mobile nodes, threats from compromised nodes within network, limited physical security, dynamic topology, scalability and lack of centralized management.

The paper has been organized as follows. Section II reviews the literatures, Section III describes Routing protocols of MANET, Section IV explores the Challenges of MANET. Section V discusses the different types of attacks and Section VI describes the various defense mechanisms. Section VII concludes the paper. Finally Section VIII lists the Refenrence.

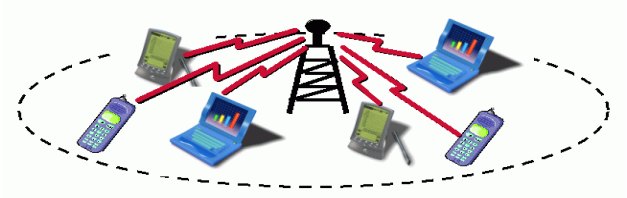

Figure 1.MANET with heterogeneous devices

II. LITERATURE REVIEW

In [1] the author discusses the various kinds of routing protocols. Major classifications are *Proactive, Reactive and Hybrid* protocols. According to [2], MANET facing large number of challenges like scalability, routing, Quality of Service, security, energy conservation, node cooperation and interoperation.

An ad hoc network can be subject to many types of attacks. Various types of attacks in different layers of network protocol stack have discussed in [3].

Reputation-based Internet protocol security [4] provides layered security framework and more comprehensive security solution. External threats can be avoided by using encrypted links and encryption-wrapped nodes while internal threats are detected by behavior grading.

A mechanism discussed in [5] helps to detect a range of attacks and provides an effective response with low network degradation. A game-theoretic intrusion detection model [6] increases the effectiveness of intrusion detection system and catch and punish the misbehaving node.

The framework explored in [7] is used to enforce cooperation between nodes to avoid selfishness of network nodes. The security aware ad-hoc routing(SAR) [8] is able to find a route with a quantifiable guarantee of security. If one or more routes that satisfy the required security attributes SAR will find the shortest such route. If all the nodes on the shortest path satisfy the security requirements, SAR will find routes that are optimal.

A Network performance centric design scheme was introduced in [9] and proposed adaptive problematic nodes filtration method to localize the anomaly nodes.

III. ROUTING PROTOCOLS OF MANET

Numerous protocols have been developed for ad hoc mobile networks to handle multi-hop network topology and mobility. Such protocols must deal with the typical limitations of these networks, like high power consumptions, low bandwidth, and high error rates.

These routing protocols may generally categorized as

a. ***Proactive*** – maintains consistent, up-to-date routing information from each node to every other node in the network. Destination Sequenced Distance Vector(DSDV) and Wireless Routing Protocol(WRP) are examples for proactive routing protocol.

b. ***Reactive*** - creates routes only when a node require a route to a destination. Once a route has been discovered and established, it is maintained by some form of route maintenance procedure. Examples are Ad hoc On-Demand Distance Vector routing(AODV) and Dynamic Source Routing(DSR)

c. ***Hybrid*** – Incorporating the merits of Reactive and Proactive protocols. Zone Routing Protocol(ZRP) is a hybrid routing protocol

IV. CHALLENGES OF MOBILE AD HOC NETWORKS

MANET has become one of the most important areas of research in the recent years because of the challenges it pose to the related protocols. The topics that need to be resolved are as follows:

A. Scalability:

Most of the applications which are anticipated to benefit from the Ad hoc technology take scalability as granted. However, it is unclear how such large networks can actually grow. Ad hoc networks suffer, by nature, from the scalability problems in capacity. Route acquisition, service location and encryption key exchanges are just few examples of tasks that will require considerable overhead as the network size grows. Therefore, scalability is a boiling research topic and has to be taken into account in the design of solutions for Ad hoc Networks

B. Routing:

Routing in wireless Ad hoc networks is nontrivial due to highly dynamic environment. An Ad hoc network is a collection of wireless mobile nodes dynamically forming a temporary network without the use of any preexisting network infrastructure or centralized administration. In a typical Ad hoc network, mobile nodes come together for a period of time to exchange information. While exchanging information, the nodes may continue to move, and so the network must be prepared to adapt continually to establish routes among themselves without any outside support.

C. Quality of Service:

The heterogeneity of existing Internet applications has challenged network designers who have built the network to provide best-effort service only. Qualities of Service (QoS) aware solutions are being developed to meet the emerging requirements of these applications. QoS has to be guaranteed by the network to provide certain performance for a given flow, or a collection of flows, in terms of QoS parameters such as delay, jitter, bandwidth, packet loss probability, and so on. QoS in Ad hoc networks is still an unexplored area. Issues of QoS in robustness, QoS in routing policies, algorithms and protocols with multipath, including preemptive, priorities remain to be addressed.

D. Security:

A vital issue that has to be addressed is the Security in Ad hoc networks. Applications like Military and Confidential Meetings require high degree of security against enemies and active/passive eavesdropping attacker. Ad hoc networks are particularly prone to malicious behavior. Lack of any centralized network management or certification authority makes these dynamically changing wireless structures very vulnerable to infiltration, eavesdropping, interference, and so on.

E. Energy Conservation:

Energy conservative networks are becoming extremely popular within the Ad hoc networking research. Energy conservation is currently being addressed in every layer of the protocol stack. There are two primary research topics which are almost identical: maximization of lifetime of a single battery and maximization of the lifetime of the whole network. As to the device power consumption, the primary aspect are achieving energy savings through the low power hardware development using techniques such as variable clock speed CPUs, flash memory, and disk spin down. However, from the networking point of view, our interest naturally focuses on the device's network interface, which is often the single largest consumer of power. Energy efficiency at the network interface can be improved by developing transmission/reception technologies on the physical layer.

F. Node cooperation:

In MANETs, all routing protocols assume that nodes provide secure communication. But some nodes may become malicious nodes which disrupt the network operation by changing routing information etc.

G. Interoperation:

The self-organization of Ad hoc networks is a challenge when two independently formed networks come physically close to each other. This is an unexplored research topic that has implications on all levels on the system design. When two autonomous Ad hoc networks move into same area the interference with each other becomes unavoidable. Ideally, the networks would recognize the situation and be merged. However, the issue of joining two networks is not trivial; the networks may be using different synchronization, or even different MAC or routing protocols. Currently, routing, power management, bandwidth management, radio interface, attacks and security are hot topics in MANET research. Recent wireless research indicates that the wireless MANET presents a larger security problem than conventional wired and wireless networks.

V. TYPES OF ATTACKS

Security attacks can be classified as *Passive attacks* and *Active attacks*. The Passive attacks does not affect the network operation and not alter the data transmitted within the network. They attempt to capture the data.

An Active attacks are severe attacks which are performed by attackers for replicating , modifying and deletion of exchanged data. They try to change the behavior of the protocols. These attacks meant to degrade or prevent the message flow among nodes. Active attacks can again divided into two categories as : i)Internal attacks ii)external attacks

External attacks are carried out by nodes that do not belong to the network. These attacks can be prevented by using standard security mechanisms such as encryption techniques and firewalls.

Internal attacks are carried out by compromised nodes that are actually part of the network. Since the attackers are already part of the network as authorized nodes, internal attacks are more severe and difficult to detect when compared to external attacks.

A. Attacks in Different Layers:

a. Attacks at Physical layer:

Physical layer attacks are hardware oriented. They need support from hardware resources. These attacks are simple to execute compared to others. There are three types of physical layer attack : i)Jamming ii)Eavesdropping iii) Active interference

b. Attacks at Data Link layer:

Data Link layer attacks affect the data transmission, operations of node and linkage between nodes etc. They can be classified as i)Selfish misbehavior ii) Malicious behavior and iii) Traffic analysis

c. Attacks at Network layer:

In MANET each node can take routing decision to forward packets, so it is easy to malicious nodes to insert themselves as member of active path from source to destination. The malicious nodes can then absorb traffic and create congestion. These network layer attacks are categories as i)Black hole ii)Worm hole iii) Gray hole iv)Sink hole v)Rushing attack and vi) Sybil attck.

d. Attacks at transport layer:

In this type the malicious node spoof the victim's IP address, find the sequence number expected by the target node and start flooding attack. Example for these attacks are i)Session hijacking ii) SYN flooding attack.

e. Attacks at Application layer:

These kind of attack to try to capture data , application and resources which in application layer. Malicious code attack like viruses, worms,spy wares and Trojan horses are example for this kind of attack

f. Multilayer attacks:

Some attacks can occur in more than one layer they are i)Modification ii)Fabrication iii)Denial of service iv)Reply

VI. DEFENSE MECHANISMS

A. Reputation-based Internet protocol security:

In this method sender and relay nodes monitor downstream nodes to confirm if packets are received and acknowledged. The Reputation Index(RI) will be incremented for downstream nodes after receiving the acknowledgement by upstream nodes. The RI values are decremented when upstream nodes do not receive acknowledgement from a downstream node within a stipulated time period. If a sender does not receive an acknowledgement, the route is broken and deleted from the route cache.

Every node calculates and maintains its own perception of every other node's reputation in a local RI index table. Any node that has a negative RI will be considered un trusted and will not be included when generating a route to a receiver. Conversely, a node with a non-negative RI is trusted and will be considered in routing process. If there are multiple paths from sender to receiver then some of the paths may be discarded depending on the sender's RI table value of nodes within those paths.

B. Intrusion detection and adaptive response mechanism:

This mechanism for MANETs detects a range of network layer attacks such as black hole, gray hole, rushing attacks etc. and also adaptively respond to the detected attacks to halt the attack and/or mitigate the damage caused by the attack and prevent further attacks from the intruding nodes. The IDAR works by adaptively selecting the intrusion response action based on the level of confidence in the detection of the attack, the attack severity and the degradation in network performance. The use of decision table to represent the intrusion response action selection criteria allows a flexible approach to management of threats and can accommodate the different security requirements of the network.

C. Game-theoretic intrusion detection model:

This unified framework initially balances the resource consumption among all the nodes and thus increase overall lifetime of a cluster by electing truthfully and efficiently the most cost efficient node known as leader. The checker catch and punish a misbehaving leader that monitor the behavior of the leader. A cooperative game-theoretic model is used to analyze the interaction among checkers. By formulating a zero-sum non-cooperative game between the leader and intruder detection service is effectively executed. The game can be solved by finding the Bayesian Nash Equilibrium where the leader's optimal detection strategy is determined.

D. Collaborative reputation mechanism:

The Collaborative Reputation Mechanism to Enforce node cooperation(CORE) is a framework based on reputation to enforce cooperation among MANET nodes to prevent selfish behavior. Each network node keeps track of other nodes' collaboration using their reputation. The reputation is calculated based on various types of information on each node's rate of collaboration. Since there is no incentive for a node to maliciously spread negative information about other nodes. Three types of reputation are used : subjective, indirect, and functional.

CORE does not use encryption for the protection of data or nodes. It does use behavior grading based on nodes' ability to participate in the routing process and the ability to

relay packets, but it is susceptible to many well-known MANET attacks

E. Security aware ad-hoc routing:

The security aware ad-hoc routing protocol is based on on-demand protocols. In SAR, a security metric is added into the route request packet and a different route discovery procedure is used. Relay nodes receive a route request packet with a particular security metric or trust level. If the security metric or trust level is not satisfied the relay node will drop the request packet. If they are satisfied it sent the packets to its neighbor nodes. Receiver node send a route replay with the required security metric when a path with security attributes is found.

A malicious node has the shared key used for encryption compromises the security of entire network

F. Energy-aware and self-adaptive anomaly detection scheme:

This was achieved by introducing a network performance centric design scheme for resource constrained MANETs. The scheme uses network tomography , a new technique for studying internal link performance based solely on end-to-end measurements. A novel spatial-time model to identify the MANET topology was presented. An adaptive problematic nodes filtration method to localize exactly the anomaly nodes was also implemented.

VII. CONCLUSION

This paper describes about the MANET, the challenges of MANET. Due to some loopholes there are variety of threats in ad hoc network, and this paper discussed different types of attacks. Here various defense mechanisms are summarized and Table 1 shows the comparison of different defense methods.

VIII. REFERENCES

[1]. Aarthi, Dr. S. S. Tyagi," Study of MANET: Characteristics, Challenges, Application and Security Attacks", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 5, May 2013 ISSN: 2277 128X

[2]. Rajni Sharma, Alisha saini, "A study of various security attacks and their countermeasures in manet", International journal of advanced research in Computer Science and Software Engineering", Volume-1, Issue-1, December-2011.

[3]. Gagandeep, Aashima, Pawan Kumar ," Analysis of Different Security Attacks in MANETs on Protocol Stack A-Review" International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-1, Issue-5, June 2012

[4]. T.H.Lacey,R..Mills,B.E.Mullins,R.A.Rains,M.E.Oxley,S.K. Rogers "RIPsec-Using reputation-based multilayer security to protect MANETs" ,Elsevier journal of Computer and security, September 2011

[5]. Adnan Nadeen, Michael P.Howarth, "An intrusion detection & adaptive response mechanism for MANETs", Elsevier journal of Ad Hoc Networks, September 2013

[6]. Hadi Otrok, Noman Mohammed, Lingyu Wang, Mourad Debbadi, Prabir Bhattacharya,"A game-theoretic intrusion detection model for mobile ad hoc networks", Elsevier journal Computer communications,October 2007

[7]. Michiardi P,Molva R.CORE; a collaborative reputation mechanism to enforce node cooperation, 6th IFIP CMS Conference 2002

[8]. Yi S, Naldurg P, Kravets R,"Security – aware ad routing for wireless networks", 2nd ACM international Symposium on mobile ad hoc networking & Computing.2001

[9]. Wei Wang, Huiran Wang, Beizhan Wang, Yaping Wang, Jiajun Wang,"Energy-aware and self-adaptive anomaly detection scheme based on network tomography in mobile ad hoc networks" ,Elsevier journal of Information Sciences, August 2012

Table 1 Comparison of different fortification mechanisms

S.No	Mechanism	Protocol used	Clustering	Performance metrics	Advantages	Limitations
1	Reputation-based Internet protocol security	DSR	NO	Total route errors Load Throughput	Effective at mitigating 12 attacks It provide multilayer security	Power and energy overhead. Does not mitigate bad-mouthing attack . Low routing maintenances
2	Intrusion detection and adaptive response mechanism	AODV	NO	Network performance Network traffic	High success and low false alarm rate in a range of attacks Completely isolate the intruding node for sever attacks Minimum overhead on the network	Does not consider physical or data link layer attacks
3	Game-theoretic intrusion detection model	BGP	YES	Packet analysis Energy level of node Probability of detection	Maximize the probability of detection	Quantitative approach is not followed to rate the leader.
4	Secure aware ad-hoc routing	AODV and DSR	NO	Simulation time Path discovery Route message overhead	Routes discovered by SAR come with "quality of protection" guarantees	A malicious node has the shared key used for encryption compromises the security of entire network

5	Energy-aware and self-adaptive anomaly detection scheme	AODV, DSR and DSDV	YES	Average processing time Average processing power Throughput	Monitor the spatial-time behavior of MANETs including network topology, link performance and network security	Scalability not considered and no signaling protocol