Review and Analysis of the Security Issues in MANET

Preeti Gulia
Department of Computer Science and Applications
Maharshi Dayanand University,
Rohtak, Haryana-124001

Sumita Sihag
M-Tech student of Department of Computer
Science and Applications Maharshi Dayanand
University,Rohtak, Haryana-124001

ABSTRACT

Mobile Ad-hoc Networks (MANETs) are one of the fastest emerging networks. MANET is a unstructured network in which nodes are mobile. This mobility may leads to insecurity in MANET. BFOA (Bacterial foraging optimization algorithm) is a Bio-inspired Algorithm. This algorithm simulates behavior of bacteria that can be effectively applied in various fields. This paper discusses various attacks and their prevention technique in MANET. This paper also reviews Bacteria foraging optimization algorithm and how it can be applied to secure the MANET.

KEYWORDS

Manet, Bfoa, Ids, Security.

1. INTRODUCTION

An ad hoc network is an autonomous system of mobile nodes connected by the wireless links. MANET is infrastructure less, self organizing, and self establishing wireless network. It is dynamic in nature due to topology changes every time. Nodes participating in networking are independent and can freely move. They act as host as well as router. MANET can be established anytime, anywhere; where no network approach is possible, it can be implemented [2][3]. All nodes cooperate in order to dynamically establish and maintain routing in the network, forwarding packets for each other to allow communication between nodes not directly within wireless transmission range. Rather than using the periodic or background exchange of routing information, an on-demand routing protocol is one that searches for the attempts to discover a route to some destination node only when a sending node originates a data packet addressed to the node. For transferring of data from node to node there is a mechanism of route discovery and route recovery. In order to avoid the need for such a route discovery to be performed before each data is sent, an on-demand routing. Protocol must cache routes previously discovered [4]. Various applications of MANETs are disaster relief, war field, urgent business and in military etc.

2. ATTACKS

A survey of available attacks reveals a list of MANET attacks, both applied and theoretical. These attacks are based on the specific characteristics. Attack may be of active or passive in nature.

The following are some most happening attacks on MANET networks.

i) **Black Hole-** This attack is a kind of denial of service, where an attacker node attracts all packets by falsely advertising a shortest path to the destination node and creates a reply containing shortest path before reaching actual node reply, whose packets it wants to intercept and, then, absorb them without forwarding to the destination [10]. In this way a fake route gets created. Attacker shows itself as an established node in the network topology and make complete refusal to actual node to participate in the network, this may cause a denial-of-service and or may be man-in-the middle attack. This type of attack is difficult to detect in MANETs and most affecting attack among attacks.

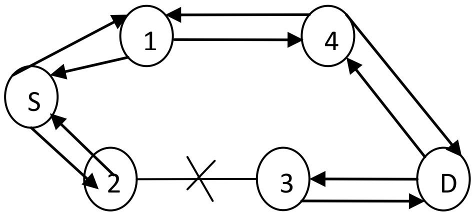

Fig 1: Black hole attack

ii) Gray Hole / Selective Forwarding– This attack is a variation of the black hole attack, where the attacker node is not initially infected; it turns malicious or infected sometimes later. In this attack, an attacker drops all data packets except control messages to route through it. An attacker node established in routing topology, selectively drops packet causing network disruption. This attack is difficult to detect. This type of attack is challenging to find in terms of type of data and drop rate of packets [7]. An attacker node can participate fully in route discovery, inserting itself into the topology, can selectively drop data packets at a low rate, but slightly increase in loss rate can cause a serious degrade in performance. An overloaded node, without fault of its own, might selectively drop packets, thus behaving like a Gray Hole.

iii) Route Error Falsification– In this attack, if destination node or an intermediate node moves along an active path, node also invalidates the route for this destination in its routing table by sending false route error messages [6]. Nodes can generate false route error messages instead of transporting data messages. This delays a packet delivery and can force the sending node to request a node discovery.

iv) Short Circuit/replay- This type of attack does not require authentication, only having the ability to read and rebroadcast messages. Malicious node records old valid messages of other nodes and resends them later [8]. This results in other nodes with updating routing table with stale or altering routes. These attacks are later misused to disturb the routing operation in a MANETs.

v) Sinkhole- In sinkhole Attack, a malicious node advertises wrong routing information to produce itself as an authenticated node and capable of receiving whole network traffic. After receiving whole network traffic it modifies the secret information. This attack can be difficult to find because all routing may be handled by nodes without disruption.

vi) Wormhole– In this attack, a malicious node captures packet from one location or from one malicious node in network and "tunnels "these

vii) packets at another location or to the other malicious node, the second malicious node replay the "tunneled" packets locally. The tunnel exist between two malicious nodes is referred to as a wormhole. Wormhole attacks are severe threats to MANET routing protocols. Attackers use wormholes in the network to make their nodes appear more attractive so that more data is routed. The wormhole can drop packets by short-circuiting the regular flow of routing packets or to avoid detection, it can carefully forward packets [9].

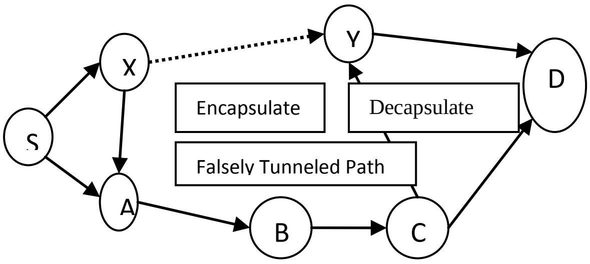

Fig 2: Wormhole Attack

Some of these attacks result from normal behavior of nodes within a system. Black and Gray Hole attacks can result from non-malicious behavior on the part of nodes. Route Error Falsification and Selective Drop can be difficult to differentiate.

1.1. Threats

Many attacks can cause threats; understanding how these attacks function allows for better placement of preventive mechanisms. Multiple attacks that can be classified under multiple threat types. Rushing uses the mechanism of relay with the intent to deny a packet / denial of service. Sinkhole may not be disruptive and thus pose no threat but it does create a future vulnerability in the network to a denial of service if the Sink Hole node produces another attack .Eavesdrop, masquerade and modification attacks may also cause threats. Sometimes these attacks are classified into the following threat types:

2.1.1 Denial of Service: A denial-of-service attack intended to deny or delay service to authorized persons. The nodes may be a single node or the whole network / group.

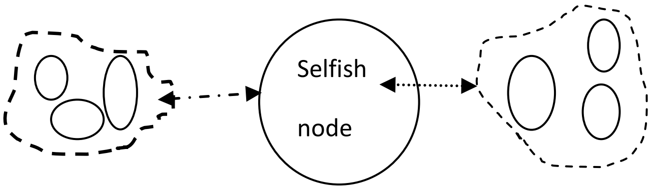

Fig 1: Denial of Service Attack

2.1.2) Traffic Analysis: Viewing information about network topology, nodes location, roles played by nodes, sizes, timings to gather insight into network topologies and able to gain confidential information. Each of these attack classifications can be considered a threat against a specific set of vulnerabilities already identified for the given assets.

3. PREVENTION TECHNIQUES

There are some of the prevention techniques which when applied can lead to the secure and the better results for the transferring of the data from source to the destination.

a. Secure Routing

In the routing protocols, authentication techniques helps to avoid many of the attacks described above. The nodes wishing to participate in routing process guarantee that the nodes are authenticated. Trusted network elements will behave according to the protocol rules. In this way unauthorized nodes will prevent from participating in the network and prevention of occurring routing attacks. Authentication can be based either on public-key or symmetric cryptography. In the former case, nodes issue digital signatures associated with the routing messages. Signatures can be verified by any other node [1][12], providing a secure proof of the identity of the sender. Three solutions analyze the exiting solutions; these solutions are based on symmetric cryptography, asymmetric cryptography and hybrid solution. Symmetric cryptography solutions include SRP (Secure routing protocol) helps to provide security in MANETs. Secure efficient Ad-hoc distance vector (SEAD) routing: These helps to provide security in an efficient way and the third protocol is Arianne. Asymmetric cryptography solutions have two protocols. Authenticate routing for ad-hoc network (ARAN) and Security aware Ad-Hoc Routing (SAR). Hybrid solutions include Secure Ad-hoc on-demand Distance Vector (SAODV) and secure link-state routing protocol (SLSP). Similar properties can be constructed using secret-key cryptography, such by using MACs (Message Authentication Codes) similar properties obtain using secret key cryptography [5][14]. Key management is hard task in MANETs than in wired networks due to the lack of any infrastructure or central control. Services such as certification authorities (CA) or key servers (KS) cannot be placed obviously, and the majority of the solutions proposed so far based on schemes. The whole key management system is spread out to a subset of the mobile nodes. This scheme having mostly distributed key agreement protocols, like two parties Diffie-Hellman (DH).

The basic protocol extended towards n-party versions, in such a way that n nodes can establish a common key for group communications. Encrypted Key Exchange (EKE) protocols have also applied in MANETs. These schemes have goal of allowing two parties to generate a long-term common key from a shared password.

b. Intrusion Detection System (IDS)

An intrusion detection system (IDS) is a part of security system that detects unwanted activities, security violations to systems [1][11]. Each mobile node runs an IDS agent independently that has to observe the behaviour of neighbouring nodes, detect local intrusion, Cooperate with neighbouring nodes, make decisions and take actions. By monitoring security policy, system activities and response to those are apparently intrusive. If an attack is identified once in the network, a response can be initiated to prevent or minimize the damage to the system. An IDS also provides information about intrusion techniques, enhancing our understanding of attacks and informing our decisions regarding prevention. Although there are many intrusion detection systems for wired networks, they do not find simple application to MANETs. For improving security, Enhanced Intrusion Detection System for discovering affected or attacker nodes in Mobile Ad Hoc Networks: The main feature of this system is its ability to discover malicious nodes which can partition the network by falsely reporting other nodes as misbehaving and then proceeds to protect the network.

4. PROPOSED WORK

MANET (Mobile ad-hoc network) is an autonomous and fast emerging network system. MANET is infrastructreless, self organizing, and self establishing wireless network. It can be established anytime, anywhere. It provides a possibility of creating a network where creation of fixed infrastructure is not possible, here MANET can be implemented. It has various applications like military, disaster relief, war field, urgent business etc. Security in MANET is important issue due to its wireless nature. Lack of infrastructure, lack of physical and network layer security makes MANET network insecure. For providing network various routing protocol are used. The security of these protocols is compromised by the various types of attacks. This paper discuss that how these attacks affect the routing protocols in MANETs. In wired network, security implementation is easier and more reliable than wireless network. Security is challenging and difficult task in MANET. Here it is difficult to separate inside network from outside network, no single security solution is enough due to dynamic nature, topology changes every time in network. Traditional routing algorithms such as distance-vector and link-state algorithms that are used in fixed networks cannot be directly applied to mobile ad hoc networks. The constraints of MANETs demand the need of specialized routing algorithms that can work in a decentralized and self-organizing way. The routing protocols of a MANET must dynamically adapt to the variations in the network topology. For providing security there are various protocols, these provide security better but not very successful. So improving the security bio-inspired techniques are used, which solves security problems. They are more robust, reliable, and scalable than other conventional routing algorithms. The main characteristics of these techniques are self organizing, dynamic and capable of finding alternative path.

5. BFOA

The technique BFOA (bacterial foraging optimization algorithm) is new comer to the biological techniques. The process, in which a bacterium moves by taking small steps while searching for nutrients, is called chemo taxis and key idea of BFOA is mimicking chemo tactic movement of virtual bacteria in the problem search space, individual bacterium communicate to other by sending signals [13]. It is a global optimization algorithm for various optimization problems. This technique is also inspired by the social foraging behavior like ant colony and particle swarm optimization. It attracts the researchers due to its efficiency in solving real world optimization problems and gives better results than traditional methods of problems solving. The next section explains that how BFOA can be applied in MANET to detect and prevent from BLACKHOLE attack.

This algorithm consists of three phase to detect and prevent from BLACKHOLE attack in MANET.

Phase 1: Network Construction phase

1. Create network consisting 25 nodes.
2. Select source and the destination node.
3. The transmission will start from source to destination by multi hop.

Phase 2: Detection of attack

1. The blackhole attack is detected in the network by the chemotactic movement of data in the network.
2. The node that is not transmitting the data forward is the blackhole node.

Phase 3: Recovery

1. In the elimination mode of BFOA, eliminate the blackhole node.
2. In the dispersion and reproduction phase, a node is generated that is the replacement of blackhole node.
3. Analyze the P.D.R, throughput and the routing overhead.

6. CONCLUSION

Blackhole attack in MANET can degrade the performance of network to a greater extent, because this attack is very savior to MANET as it absorbs all the packets of data and doesn’t forward these packets to further nodes. This paper describes the BFOA technique to detect and prevent from blackhole attack. In future, this technique can be simulated on NS2.

7. REFERENCES

[1] Sevil Şen, John A. Clark, Juan E. Tapiador, in Security Threats in Mobile Ad Hoc Networks.

[2] internet Engineering Task Force MANET Working Group. Mobile Ad hoc networks (Manet) Charter Available at http:// www.ietf.org/html.charters/manet-charter.html.

[3] Asis Nasipuri, Mobile Adhoc networks,Department of Electrical and Computer Engineering, The university of North Carolina at charlotte.Charlotte,NC 28233-0001

[4] Mr. Rajneesh Kumar, Dr. Anil Kapil, An Efficient Searching and an Optimized Cache Coherence handling Scheme on DSR Routing Protocol for MANETS, in IJCSI Vol 8, Issue 1, Jan 2011.

[5] M. Steiner, Tsudik G., and Waidner M., "Diffie-Hellman Key Distribution Extended to Group Communication", In Proc of the ACM Conference on Computer and Communication Security, pp. 31-37, 1996.

[6] Antonio Martin Boston University Conference on Information Assurance and Cyber Security, "A Platform Independent Risk Analysis for Mobile Ad hoc Networks"2006.

[7] Gagandeep, Ashima, Pawan kumar, Analysis of different security attacks in MANETs on protocol stack, in IJEAT Vol1, issue 5, 2012.

[8] Ankita Gupta, Sanjay Parkash Ranga, various routing attacks in mobile Ad-Hoc networks, at http\\ www.ijccr.com, Vol 2, issue 4, 2012

[9] Abhay kumar Rai, Rajeev Ranjan Tewari, Saurabh Kant Upadhyay, Different types of attacks on integrated MANET internet communication in IJCSS, Vol 4 Issue 3 .

[10] K.Sahadevaiah, Department of computer science and engineering, Impact of security attacks on a new security protocol for mobile Ad-Hoc networks, 2011.

[11] Zaiba Ishrat, Security issues, challenges & solution in MANET in IJCST Vol 2, Issue 4, oct-nov 2011.

[12] kuldeep Sharma, Neha Khandelwal, Parabhakar. M, An overview of security problems in MANET.

[13] Swagatam Das,Sambarta Das Gupta, Arijith Abraham, Senior member,IEEE, and Amit Kanas,meber IEEE, Vol 39, May 2009.

[14] Bing Wu Jianmin Chen, Jie Wu, Mihaela Cardei, A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks in Springer 2006.