International Journal of
Emerging Research in Management &Technology
ISSN: 2278-9359 (Volume-4, Issue-12)

Research Article | **December 2015**

Danger Theory Based Model to Prevent Sleep Deprivation Attacks in MANETs

Manish Poonia[1], Gajanand Sharma[2]

[1] Research Scholar, Suresh Gyan Vihar University, Jaipur, Rajasthan, India

[2] Associate Prof, Suresh Gyan Vihar University, Jaipur, Rajasthan, India

Abstract:

Mobile Ad-Hoc Networks (MANETs) are one of the most commonly used network services these days. They play a great role in tactical situations such as disaster relief or battle fields, making it an important area for research. But, unfortunately, the very factors that make MANETs (elective resilience, and decentralization) pose tremendous challenges for those tasked with securing such environments. Various types of attacks are possible on MANETs. Sleep deprivation attack is one of them. Our objective is to design an artificial immune system to secure from sleep deprivation attack and is based on biological Danger Theory. The basic problem is to identify the threat in any incoming packet based on the database and the properties / behaviour of the packet. To do this we would design an algorithm to classify and analyse the packets. The algorithm takes a packet as input, based on the parameters and header of the packet, the packet is analysed and using the database of previous dangerous and alarmed packets the classifier would classify the packets into 5 categories. The packets belonging to rest two categories are accepted, belonging to latter two are discarded and to that of last are alarmed. Our system is divided into 2 subsystems viz. analysing subsystem and adaptive subsystem. The analysing subsystem analyses the packet based on its header and forwards the packet along with its pattern to the adaptive subsystem. The adaptive subsystem searches the pattern of a packet in its database and decides whether to accept or reject the packet. The adaptive subsystem would be also responsible for updating the databases.

Keywords: MANET, Ad-hoc Network, packet, analyses, sleep depriving attack

I. INTRODUCTION

A MANET is a collection of mobile nodes which can self-organize freely and dynamically into arbitrary and temporary network topologies. It consists of mobile platforms (e.g. a router with multiple hosts and wireless communications devices) simply referred to as nodes which are free to move about arbitrarily. The nodes may be located in or on airplanes, ships, trucks, cars, perhaps even on people or very small devices, and there may be multiple hosts per router. A MANET is an autonomous system of mobile nodes. The system may operate in isolation, or may have gateways to and interface with a fixed network [8].

In general, MANETs have to face issues much different from the traditional wired systems due of the lack of a centralized infrastructure. Each node in the network must either ask other nodes for a path to a destination on demand (reactive routing) or maintain a local view of the network topology for route calculation (proactive routing), which must be frequently updated. The situation becomes typically challenging and is in need of efficient management of nodes.

II. LITERATURE SURVEY

MANETs are very important type of networks used in various organizations. But MANETs are vulnerable to a number of attacks. Sleep deprivation attack is also one of them. It is basically a denial of service kind of attack in which the main aim is to drain o limited resources in the mobile ad-hoc nodes (e.g. the battery powers), by constantly making them busy processing unnecessary packets. The power resource is a very important component in case of MANETs as the nodes are continuously moving. So confronting the sleep deprivation torture is a very necessary aspect.

A. Approach

Basically, there are 2 types of approaches to deal with sleep deprivation attacks [6].

B. Hierarchical

In such an approach, we assign special privileges to some specific nodes such that they take care of the entire network. But, the system comes with its own challenges as we are not able to decide for the rights that must be given to particular nodes. Secondly, we also have to apply algorithms to choose the privileged nodes.

C. Collaborative

In such an approach, the attack is handled by the collaboration of all the nodes. The various nodes of the network stay in touch with each other such that any irregularity or discrepancy is informed to all other nodes of the system. It's a better approach to be applied in MANETs because their job is mainly conceptualized on the principle of collaboration.

D. Preferred Solution

Collaboration between nodes is the obvious solution, and has been examined by many other researchers. The Danger theory is one of the Collaboration based approach. It implies that the concentration of the danger or safe signals which come from the body tissues and caused by specific antigens control the response of the Human Immune System (HIS) to either tolerate those antigens. The same concept can be implied onto MANETs through a model based on tolerating and rejecting the packets.

The underlying idea is relatively simple. When a node ends another node misbehaving, it could tell other nodes about the problem, and then they could all avoid the problematic node. The trouble with reputation-based approaches is that they introduce new problems a node could have been misidentified as harmful, and would still be shunned, or a malicious node could lie about having been hurt, potentially crippling the network[2]. The notion of trust, as distinct from reputation was introduced to deal with this. Trust is based on most of the same information as reputation, and introduces new complications, such as whether or not to re-trust nodes that have previously been denied as malicious, and if so, when to do it, as well as what to do if malicious nodes attempt to falsely accuse good nodes of being bad.

The challenge with Artificial Immune System (AIS) is that it is very complex to understand and mitigate the Human Immune System. So, it is complicated to decide for suitable features that are to be implemented according to the need of the system. In case of MANETs also, the needs are equally complex.

III. ATTACKS POSSIBLE

The major challenges MANETs have to deal with are as follows [6]

1. In a MANET, nodes cooperate to route traffic. Any routing algorithm must contend with nodes that may be under an attacker's control.
2. Bandwidth is locally shared and often highly-constrained in a MANET. How can this congestion be handled while simultaneously detecting nodes that are maliciously flooding the network or dropping traffic.
3. Battery life is often a concern for MANET designers, as roaming nodes often wish to act slushy in order to conserve power. Thus, CPU cycles and wireless power management are extremely valuable commodities.
4. As the traffic observed by a node depends greatly on network topology, it is difficult for systems to learn what good tra c patterns look like, and what constitutes an attack.
5. Nodes frequently enter or leave the network, causing frequent changes in network membership and contributing to localized changes in topology.
6. There is no central authority for network monitoring and management, as the network can become disjoint at any time.

A. Attacks

The various challenges have lead to scope for various attacks in MANETs as listed below [8][3]

.

B. Eavesdropping

The intruder silently listens to the communication by tapping the wire-less link while other nodes have no idea about its intrusion.

C. Traffic Analysis

The intruder analyses the traffic communications in order to gain in-formation about the network topology and hence inject the attack in a strategic place (e.g. near the cluster head) that helps the threat to succeed.

D. Denial of Service

The intruder aims to over own the link by fake packets in order to make a link jam and hence down the path to the intended server to stop the service. Also, it could deplete the nodes energy such as, sleep deprivation attack or resource consumption attack.

E. Black hole

The intruder injects the control routing packets with fake information in order to attract the node that requested the route and hence gain that route. After the intruder acquires the route, the intruder could apply different types of attacks.

F. Dropping packets

The intruder simply drops a packet into the network destined for the target node. If it performs a selective dropping, it will be harder to be detected.

G. Delaying packets

In this attack, the intruder does not forward the received packets directly even if the link is empty.

H. Worm hole

In this attack, a cooperation between two intruders as a minimum is required to communicate through a high speed link to deceive the nodes that wrongly consider the malicious link as the shortest path to the destined node.

I. Sybil
In this attack, the intruder masquerades under the identity of multiple nodes.

J. Rushing
In this attack, the intruder broadcasts a route request and reply packets very quickly in order to make the nodes discard any other control packet in the network.

K. Sink hole
In this attack, the intruder attracts the nodes to use its fake route and hence it could easily inject any type of attack.

L. Detour
In this attack, the intruder creates virtual nodes on the optimal routes to appear longer and costlier than the other non-optimal routes; these forces the nodes to wrongly use the non- optimal route.

M. Exploiting node penalizing schemes
In this attack, the intruder broadcasts error messages about well per-forming nodes and causes jamming to consider these nodes to be put on the black list.

N. Routing table overflow
In this attack, the intruder overflows the nodes routing tables with fake routing information.

IV. PROPOSED WORK
The basic problem is to identify the threat in any incoming packet based on the database and the properties/behavior of the packet. To do this we would design an algorithm to classify and analyze the packets. The algorithm takes a packet as input, based on the parameters and header of the packet, the packet is analyzed and using the database of previous dangerous and alarmed packets the classifier would classify the packets. We also have a database of potentially dangerous packets whose packets are sent back to the waiting queue. We utilize the concept of minimal threshold and maximal threshold.

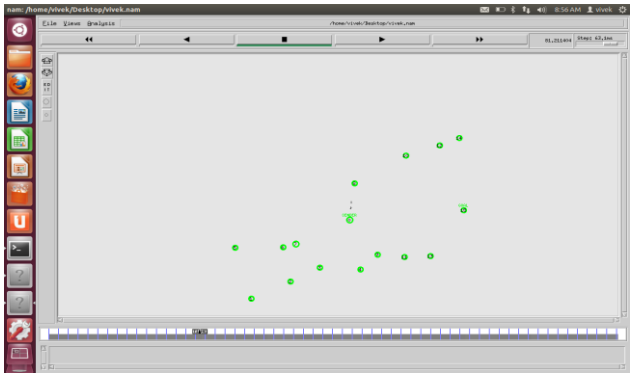

Figure: Deployment of nodes

V. FUTURE WORK
The basic assumption of our model is that the network track is categorized into these 5 classes:
A: Legitimate traffic sent by nodes
B: Legitimate traffic serviced by nodes
C: Malicious traffic sent by attackers
D: Malicious traffic serviced by vulnerable nodes
E: Malicious traffic serviced by immune nodes or lost in the network

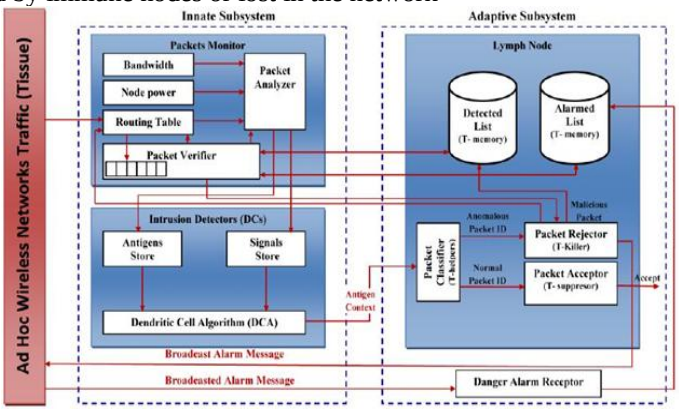

Figure: MDCA model [3]

The traffic of type A B is considered to be safe while C D are to be put into the dangerous list. The traffic of type E is to be put into the alarmed list. If the classified packet is found to be dangerous, it is rejected and its entry is made in the dangerous list of the database and a signal is generated and sent to alarmed list. If the packet is found to be in the alarmed list, it is directly discarded. If the packet is neither in dangerous list nor in alarmed list, it is accepted by the system.

Our system is divided into 2 subsystems viz. analyzing subsystem and adaptive subsystem. The analyzing subsystem analyses the packet based on its header and forwards the packet along with its pattern to the adaptive subsystem. The adaptive subsystem searches the pattern of a packet in its database and decides whether to accept or reject the packet. The adaptive subsystem would be also responsible for updating the databases.

The basic objective is to maximize the channel performance which is given by the equation:

$$= 100\ B \quad A$$

The factor will be maximum if we are able to serve more and more legitimate track.

VI. CONCLUSION

Due to dynamic topology, distributed operation and limited bandwidth MANET is more vulnerable to many attacks. In this paper, we discuss MANET and its characteristics, challenges, advantages, application, security goals, various types of security attacks in its routing protocols. Security attack can classified as a active or passive attacks. Different security mechanisms are introduced in order to prevent such network .We analyzed the attack with four different scenarios with respect to the performance parameters of end-to-end delay, throughput and network load. In a network it is important for a protocol to be redundant and efficient in term of security.

REFERENCES

[1] Ismail M. Alsaqour R. and Israf D Abdelhaq M., Hassan R. Detecting sleep deprivation attack over manet using a danger theory based algorithm. In-ternational Journal on New Computer Architectures and Their Applications (IJNCAA), 2011. 8

[2] Bentley P. Cayzer S. Kim J. Aickelin, U. and J. McLeod. Danger theory: The link between ais and ids. Springer, 2003. 7

[3] David Wagner Chris Karlof. Mobile ad hoc networks: attacks and counter-measures. Published by Elsevier Science, 2003. iv, 2, 11

[4] Ismail M. Hassan R. A suvey on mobile ad hoc network. Computer Networks, 2002. 8

[5] Bentley P. Wallenta C. Ahmed M. Kim, J. and Hailes. Danger is ubiqui-tous: Detecting malicious activities in sensor networks using the dendritic cell algorithm. Springer, 2006. 8

[6] Katherine Ho man Attila Ondi Richard Ford Marco Carvalho Derek Brown William H. Allen Gerald A. Marin. Danger theory and collaborative ltering in manets. Springer, 2008. 2, 6, 8

[7] S. Sara janovic and J.Y. Le Boudec. An arti cial immune system approach with secondary response for misbehavior detection in mobile ad hoc networks. IEEE Transactions on Neural Networks, 2005. 8

[8] Hu M. Wang, D. and H. Zhi. A survey of secure routing in ad hoc networks. 9th IEEE International Conference on Web Age Information Management, 2008. 1, 2, 8

