IJCSMS International Journal of Computer Science & Management Studies, Vol. 12, Issue 02, April 2012
ISSN (Online): 2231 –5268
www.ijcsms.com

Review of Artificial Immune System to Enhance Security in Mobile Ad-hoc Networks

Tarun Dalal[1], Gopal Singh[2]

[1]M.tech Student, Department of Computer Science and Applications,
M. D. University, Rohtak-124001, Haryana, India
tarundalal88@gmail.com

[2]Assistant Professor, Department of Computer Science and Applications,
M. D. University, Rohtak-124001, Haryana, India
gsbhoria@gmail.com

Abstract

Mobile Ad-hoc Networks consist of wireless host that communicate with each other. The routes in a Mobile Ad-hoc Network may consist of many hops through other hosts between source and destination. The hosts are not fixed in a Mobile Ad-hoc Network; due to host mobility topology can change any time. Mobile Ad-hoc Networks are much more vulnerable to security attacks. Current research works on securing Mobile Ad-hoc Networks mainly focus on confidentiality, integrity, authentication, availability, and fairness. Design of routing protocols is very much crucial in Mobile Ad-hoc Network. There are various techniques for securing Mobile Ad-hoc Network i.e. cryptography. Cryptography provides efficient mechanism to provide security, but it creates very much overhead. So, an approach is used which is analogous to Biological Immune System, known as Artificial Immune System (AIS). There is a reason of AIS to be used for security purposes because the Human Immune System (HIS) protects the body against damage from an extremely large number of harmful bacteria, viruses, parasites and fungi, termed pathogens. It does this largely without prior knowledge of the structure of these pathogens. AIS provide security by determining non-trusted nodes and eliminate all non-trusted nodes from the network.

Keywords: *Ad- hoc, MANET, Cryptography, Artificial Immune System.*

1. INTRODUCTION

Mobile Ad-hoc Network (MANET) - A Mobile Ad-hoc Network (MANET) is a wireless network that can be formed without any pre-existing infrastructure in which a node can act as a router and a host A MANET is an autonomous system of mobile routers connected by wireless links. In MANETs, topology may change rapidly and unpredictably, since the routers are free to move randomly and organize themselves arbitrarily. There is no fixed infrastructure in MANET. Such networks are envisioned to have dynamic, sometimes rapidly-changing, random, multi-hop topologies which are likely composed of relatively bandwidth- constrained wireless links.

MANET Routing - Ad-hoc wireless networks provide direct peer-to-peer communication between nodes without the need for any infrastructure (hubs, access points etc.), where source and destination are out of range of one another, packets may be forwarded by one or more intermediate nodes. In the simplest system, every node broadcasts its neighbors list from time to time, and a source sends the packet to a forwarder that has the required destination on its neighbors list. This can be extended to more than two hops by using the shortest route based on hop-count. This does not always lead to the selection of the best route when there is a choice. A better approach may be to try to minimize the number of medium access attempts along the entire route (e.g. by choosing hops based on their previous probability of success).
Probability of success depends on two different factors:

1. The signal strength depends upon the length of hop.
2. Interference depends on the traffic congestion around the receiving node.

Routing can be of two types: Re-active routing and Pro-active routing.

MANET Routing Protocols - MANET routing protocols can be categorized as two types of protocols:
1) Table-driven/pro-active routing protocols
2) Source-initiated (demand driven) routing protocols

Table driven routing protocols – These protocols attempt to maintain consistent, up-to-date routing information from each node to every other node in the network. In these protocols, each node maintain one or more tables to store routing information, and they respond to changes in network topology by propagating updates throughout the network in order to maintain a consistent network view

On Demand Driven Re-active Protocols- On demand protocols create routes only when desired by source nodes. When a node requires a route to destination, it initiates route discovery process within the network. Once a route is discovered and established, it is maintained by route maintenance procedure until either destination becomes inaccessible along every path from source or route is no longer desired.

Routing Attacks in MANET -MANET has no clear line of defense, so it is accessible to both legitimate users and malicious attackers. In the presence of malicious

IJCSMS International Journal of Computer Science & Management Studies, Vol. 12, Issue 02, April 2012
ISSN (Online): 2231 –5268
www.ijcsms.com

nodes, one of the main challenges in MANET is to design the robust security solution that can protect MANET from various routing attacks. In MANET different routing attacks, such as flooding, black hole, link spoofing, wormhole, and colluding misrelay attacks, as well as existing solutions to protect MANET protocols. The malicious nodes can attacks in MANET using different ways, such as sending fake routing information fake messages several times and advertising fake links to disrupt routing operations.

Types of Attacks in MANETs: Flooding Attack, Black hole Attack, Link Spoofing Attack, Wormhole Attack, Colluding Misrelay Attack.

Security Techniques- In MANETs, security is a Major issue because of there is no clear line of defense and lack of infrastructure. So, topology changes rapidly. There are various security techniques that are used for providing security in wireless networks**.**

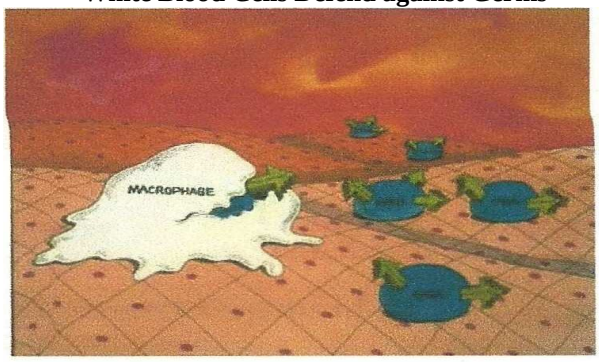
1) Cryptography
2) Public Key Cryptography
3) Private Key Cryptography
4) Trust based models
5) Collaborative techniques for Intrusion Detection

All these techniques introduce much overhead which is not required because of bandwidth constraint limitation in MANETs. There is another technique which has been used in my dissertation which is Artificial Immune System (AIS). AIS provide security by a method which is analogous to Biological Immune System (BIS). AIS is used because of two reasons: Firstly, the BIS provides the human body with a high level of protection from invading pathogens in a robust, self-organized and distributed manner. Secondly, current techniques used in computer security cannot cope with dynamic and increasingly complex nature of Ad-hoc networks and their security.

Biological Immune System-

The BIS is a system of biological structures made up of special cells, proteins, tissues, and organs, that work together to protect the body against germs and pathogens every day. It detects a wide variety of antigens, from viruses to parasitic worms, and needs to distinguish them from the organism's own healthy cells and tissues in order to function properly. BIS does a great job of keeping people healthy and also preventing infectious. The cells involved for functioning of BIS are white blood cells or leukocytes which come in two basic types that combine to seek out and destroy disease-causing organisms or substances. Leukocytes are stored in many locations of body, including bone marrow, spleen and thymus. They are also called lymphoid organs. The leukocytes circulate through the body between the organs and nodes via lymphatic vessels and blood vessels.

White Blood Cells Defend against Germs



Macrophages Identify Germs

Fig.1.12: Physiology of Primary Organs of BIS

In this way, the immune system works in a coordinated manner to monitor the body for germs or substances that might cause problems.

The two basic types of leukocytes are:

l) Phagocytes. Cells that chew up invading organisms

2) Lymphocytes. Cells that allow the body to remember and recognize previous invaders and help the body destroy them

2. OBJECTIVE

The MANET can be unsecure due to either internal or environmental factors or both. MANET faces this problem because of the undefined infrastructure. Any node can join network or disjoin network at any instant of time. Therefore, node authentication should be known before providing any services of the network to the nodes. This dissertation reaches the objective that malicious node should not get right to transfer the information within the network. To achieve this objective an approach analogous to BIS is implemented to detach good nodes from bad nodes. This approach is termed as AIS

3. LITERATURE SURVEY

1) Arun Kumar Bayyaet. al. [Kentucky University], "Security in Ad-hoc network", presented overview of existing security techniques that can be employed in Ad-hoc networks. Key management, Ad-hoc Routing and Intrusion Detection were also discussed. Key management protocols are still very expensive and not very safe to use. There is a need to make existing routing protocols more

IJCSMS International Journal of Computer Science & Management Studies, Vol. 12, Issue 02, April 2012
ISSN (Online): 2231 –5268
www.ijcsms.com

secure and robust to adapt to the demanding requirements of the MANET. Intrusion detection is also critical research area and difficult to achieve in the resource deficient Ad-hoc environment.

2) P. Yi et. al., "A New Routing Attack In Mobile Ad-hoc Network", an approach where each node monitors the RREQ it receives and maintains a count of a RREQ's received from each sender during a present time period. The RREQ from a sender whose RREQ rate is above threshold will be dropped without forwarding. Unlike this method where the threshold is fixed, this approach determines the threshold based on a statistical analysis of RREQs.

3) S. Kurosawa et. al., "Detecting blackhole attack on AODV based MANET by dynamic learning method", proposed statistical based anomaly detection approach to detect the black hole attack, based on differences between destination sequence numbers of the received RREPs. It can detect the black hole attack at low cost without introduci11g extra routing traffic, and it does not require modification of existing protocols. A location information based detection method to detect link spoofing attack by using cryptography with a Global Positioning System (GPS) and at time stamp.

4) Y-C Hu ET. al., "Wormhole attack in wireless network", proposed two types of lashes: temporal lashes and geographical lashes to defend against wormhole attack. Drawback of temporal leash is that it requires all nodes to tightly have synchronized clocks. For geographical lash, each node must know its own position and have loosely synchronized clocks. A sender of a packet includes its current position and sending time. Therefore, a receiver can judge neighbour relations by computing distance between itself and the sender of a packet. The advantage of this approach is that the time synchronization needs not to be highly tight.

5) Jungwon Kim ET. al. [2006], "Immune system approaches to Intrusion Detection- A Review", proposed the analogy between the Human Immune System (HIS) and Intrusion Detection System (IDS) naturally attracts computer scientists to research on immune system approaches to intrusion detection. The review conducted in this paper focused on providing an overview of IDS for AIS researchers to identify suitable intrusion detection research problems. Information was also provided for IDS researchers about current Artificial Immune System (AIS) solutions.

4. METHODOLOGY

This work follows the methodology that is as follows

1. Generation of MANET through MATLAB programming.
2. Implementation of AIS
3. Creating IA and sending a copy to all nodes.
4. Self/non-self-discrimination is done through IA programming in MATLAB.
5. Generation of network for AODV protocol using MATLAB

Suitability of AIS to MANET- MANETs has mobile nodes which act as router. The nodes in MANET itself are responsible for the forwarding of traffic from source nodes to destination node through intermediate nodes. Decentralization and node instability are some key features in MANETs. There are two types of attacks in MANETs, internal attack and external attack. In the internal attack, the nodes within the network can be compromised and can mislead other nodes to miss-forward the packets to the false nodes. The nodes in the MANETs can join or leave the domain without required permission, so nodes cannot be trusted. The malicious attackers are the external attackers that misroute the packets to false nodes. In human body, whenever virus enters the antibodies are produced which kills viruses. Once antibodies are produced, they continue to exist in the body and the future chance of entering the virus is completely negligible. The same process can be used in the MANET by detecting malicious nodes and compromised nodes and providing them from using the services of the MANET. The detected nodes cannot use services of MANET in future. Therefore the BIS are suitable for MANET.

Mapping BIS to Security Architecture- To map BIS to MANET mobile Ad-hoc domain is mapped with the human body. The mobile nodes present in MANET are now taken as similar to Lymph nodes in the human body.

Natural immune	*Security approach*
Body	Mobile Ad-hoc domain
Lymph nodes	Mobile nodes
Self	Normal behavior
Antigens	Sequence of normal observed patterns
Detectors	Special patterns
Antibodies	A pattern with the same format as representation of antigen

Table: Mapping Immune System to Security Architecture.

In MANETs, there can be compromised nodes and the trusted nodes. The compromised nodes are also called malicious nodes which miss-route the packets. The trusted nodes are self nodes which forward the right packet to right destination at right time. The compromised nodes which can forward wrong data and also can forward data to a node which is not destination is called non-self node. Antigens mapped with sequence of normal observed patterns. BIS is mapped with MANET to secure MANETs from malicious attacks. The system to secure MANET as security is provided by BIS in human body is called Artificial Immune System.

IJCSMS International Journal of Computer Science & Management Studies, Vol. 12, Issue 02, April 2012
ISSN (Online): 2231 –5268
www.ijcsms.com

Artificial Immune System- AIS is a beneficial method for applying security in the MANETs. As the decentralization and node instability are the key features in the MANETs and the same nature exist in the BIS. System scalability can be influenced by a system that has a centralized feature in a decentralize nature. A number of AIS have been built for a wide range of applications including document classification, fraud detection, and network- and host-based intrusion detection. For security using AIS a multi rolled agent created called Immune Agent. The agent resides on the basic node in the domain and a replica of this IA will be sent to other incoming nodes during new connection establishment.

5. CONCLUSION

Artificial Immune System (AIS) offers a relatively novel and promising paradigm to solve the problem of security in Mobile Ad-hoc Network. In this work, a comprehensive definition on the goals has been given that should be supported in anonymous routing protocols. Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. Each must forward traffic unrelated to its own use, and therefore be a router. The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic. This work presented various routing attacks and various ways to countermeasure those attacks. It addresses how AIS will be applied to MANET for securing MANETs without creating overhead.

6. FUTURE SCOPE

AI is an emerging technique for securing wireless network now a day and will grow in future. AIS will be used for security purposes in future at very advanced rate because the bandwidth is a major issue in wireless area. The AIS provides an approach for securing wireless networks with less overhead. Therefore, AIS will be used in future for detecting intrusion, malicious nodes, external attackers and other problems also.

REFERENCES

[1] Leandro Nunes De Castro, "Fundamentals of Natural Computing: Basic Concepts, and Applications" .Algorithms

[2] Anand Patwardhan, Jim Parker, Michaela Iorga. Anupam Joshi, “Tom Karygiannis, Secure Routing and intrusion Detection in Ad Hoc Networks" 3rd International Conference on Pervasive Computing and Communications (PerCom 2005), Kauai Island, Hawaii

[3] Yasir Abdelgadir Mohamed, Azween B. Abdullah, "Immune Inspired Approach for Securing Wireless Ad hoc Networks" IJCSNS Vol. 9, No.7, pp. 206-212, july 2009.

[4] Yasir Abdelgadtr Mahamed, Azween B. Abdullah, “Security Mechanisms for Manets" Journal of engineering science and technology, Vol.4, No.2 (2009) page 231-242

[5] Rashid HafeezKhokhar ET. al., "A Review of Current Routing Attacks in Mobile Ad Hoc Network s". International Journal of computer science and security, volume (2), issue (3)

[6] Bing Wu et.al., "A Survey on Attacks and Countermeasures in Mobile Ad H oc Networks" Wireless/Mobile Network Security, Springer journal, pp. 1-35,2006.

[7] K. Sanzgiriet. al., "A Secure route Protocol Proc. of IEEE International Conference on Network Protocols (ICNP), pp. 78-87, 2002

[8] S. Hofmeyr and S Forrest, "Architecture for an Artificial Immune System", Evolutionary Computation Journal Vol. 8, No.4, (2000), pp. 443-473.

[9] Robert L. Fanelli, “A Hybrid Model for Immune Inspired Network Intrusion Detection", 2008, Springer journal, pp. 107-118.

[10]Jimmy Mcgibney, Dmitri Botvich, Sasiharan Balasubramanimam, "A combined biologically andSocially inspired protocol to mitigating threats in Mobile Ad hoc Networks", 2007.

[11] ZhengYou,Jian Wang, " DJMH: A novel model to detect and isolate malicious hosts for mobile ad hoc networks" , Elsevier, 2006, pp. 660-669.

[12] Haiyun Luoet. al., "Self-securing Ad Hoc Wireless Networks", 7th IEEE Symp. On Comp. and Communications (ISCC), Taormina, 2002.

[13] Hongmei Deng, Wei Li, and Dharma P Agrawal, “Routing Security in Wireless Ad Hoc Networks", IEEE Communications Magazine October 2002.

[14] Nikos Kominos, Dimitris Vergados, and Christos Douligeris," Detecting Unauthorized and Compromised nodes in mobile Ad hoc networks", Elsevier, 2007, pp. 289-298