International Journal of Modern Engineering Research (IJMER)
www.ijmer.com Pp-21-26 ISSN: 2249-6645

An overview of security factors of routing in Mobile Adhoc Network (MANET)

P. Visalakshi[1], S. Srikanth Balaji[2]
[1]Asst. Professor (Selection Grade), Deptt. of Computer Applications, SRM University, Kattankulathur, Chennai, south India
[2]PG student, Deptt. of Computer Applications SRM University, Kattankulathur, Chennai, South India

ABSTRACT: *A Mobile Ad Hoc Network is a kind of wireless network which is a self configuring network of mobile routers connected by wireless links. Mobile Ad-Hoc Network (MANET) has dynamic topology. Self configurability and easy deployment feature of the MANET resulted in numerous applications in this modern era. The main focus of this paper is a survey of security factors and critically analyze by most of the routing protocols which are reported in the available literature. This will help in having a wider understanding of the problem domain and can also be used to develop or some new or to extend already proposed schemes. Hence MANET does not have definite topology which are intended to join in the network can come join at anytime and they leave from the network if they do not want to be with network. (ie) There is no accountability of network nodes in MANET. The absence of centralized controller will lead to a very big security issue among nodes. The main focus of this paper is survey about the security issues about the nodes.*

Keywords: *MANET → Mobile Adhoc NETworks*

I. INTRODUCTION

Mobile ad-hoc network is deployed in applications such as disaster recovery and distributed collaborative computing where routes are mostly multi hop and network hosts communicate via packet radios. Routing is one of the challenging issues in mobile ad-hoc network. Existing protocols for ad-hoc network can generally be categorized into pro-active and re-active protocols types. It is a well known fact that most of these protocols have certain because no clear and secured boundaries in this ad hoc network. It may cause the occurrences of various link attacks. These link attacks place their emphasis on the links between the nodes and try to perform some malicious behaviour to make destruction to the links.

1.1. Problems on secure Boundaries

There is no such a clear secure boundary in the mobile ad hoc network, which can be compared with the clear line of defence in the traditional wired network. This vulnerability originates from the nature of the mobile ad hoc network which causes freedom to join, leave and move inside the network. So any one can join into this network and there may be happened leakage of secret information or messages. It leads to lose our personal and high confidential data. So anyone can make the network crash or steal the data weaknesses. Some of the main problem includes Limitation. Most of the well known protocols in this area are limited to a particular scenario i.e. does not perform well in all environments. Based on the analytical studies, it is not sufficient work has been done to evaluate their performance with respect to other techniques of similar types.

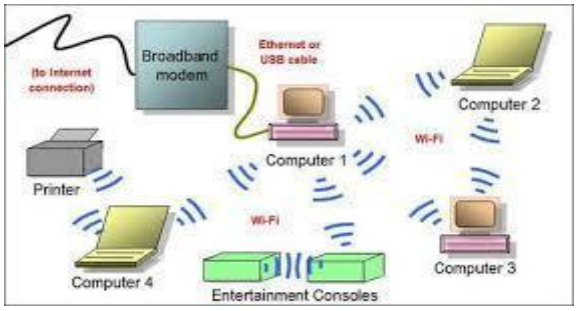

Fig1.Network with Ad hoc devices

Moreover, proposed schemes focus on routing without considering their affects on some other routing related issues.

A Mobile Ad hoc NETwork (MANET) is a system of wireless mobile nodes that dynamically self-organize in arbitrary and temporary network topologies. Peoples can thus be internetworked in areas without a pre-existing communication infrastructure or when the use of such infrastructure requires wireless extension. In the mobile ad hoc network, nodes can directly communicate with all the other nodes within their radio ranges; whereas nodes that not in the direct communication range use intermediate node(s) to communicate with each other. Due to the continuous motion of nodes, the topology of the mobile ad hoc network changes constantly. The nodes can continuously move into and out of the radio range of the other nodes in the ad hoc network and the routing information will be changing all the time because of the movement of the nodes.

A good example of this kind of threats comes from the potential Byzantine failures encountered in the routing protocol for the mobile ad hoc network.

1.2. Problems on centralized Management facility

In ad hoc network there is no centralization like server or any other devices. The absence of centralized management machinery makes the detection of attacks a very difficult problem because it is not so easy to monitor the traffic in a highly dynamic and large scale ad hoc network because of no centralisation. Some algorithms in the mobile ad hoc network rely on the cooperative participation of all nodes and the infrastructure. Because there is no centralized authority, and decision making in mobile ad hoc network this vulnerability and perform some attacks that can break the cooperative algorithm. Absence of centralisation we lost so many things like monitoring or managing the whole network. So it becomes useless for the users and chance for the hackers to steal the data.

1.3. About Battery constrained

Power supply is very important thing for on the network for communications. While nodes in the wired network do not need to consider the power supply problem because they can get electric power supply from the outlets, which generally mean that their power supply should be approximately infinite; the nodes in the mobile ad hoc network need to consider the restricted battery power, which will cause several problems. So this also the drawback for it. If the power supply will get down means we can't communicate with each other so the connections and entire network will be lost.

Fig.2. Ad hoc node security concepts

1.4. Security concepts of MANET

The major security concepts of MANET are:

- ***Availability***
- ***Confidentiality***
- ***Authenticity***
- ***Non repudiation***
- ***Authorization***
- ***Anonymity***

It is necessary to find out how we can judge if a mobile ad hoc network is secure or not, or in other words what should be covered in the security criteria for the mobile ad hoc network when we want to inspect the security state of the mobile ad hoc network. So without centralisation we cannot say whether this network is in secured manner or not.

1.4.1. Availability

The term Availability means that a node should maintain its ability to provide all the designed services regardless of the security state of it. This security criteria is challenged mainly during the denial-of-service attacks, in which all the nodes in the network can be the attack target and thus some selfish nodes make some of the network services unavailable, such as the routing protocol or the key management service. Integrity guarantees the identity of the messages when they are transmitted. Integrity can be compromised mainly in two ways

- ***Malicious altering***
- ***Accidental altering***

A message can be removed, replayed or revised by an adversary with malicious goal, which is regarded as malicious altering; on the contrary, if the message is lost or its content is changed due to some benign failures, which may be transmission errors in communication or hardware errors such as hard disk failure, then it is categorized as accidental altering.

1.4.2. Confidentiality

Confidentiality means that certain information is only accessible to those who have been authorized to access it. In other words, in order to maintain the confidentiality of some confidential information, we need to keep them secret from all entities that do not have the privilege to access them.

1.4.3. Authenticity

Authenticity is essentially assurance that participants in communication are genuine and not impersonators It is necessary for the communication participants to prove their identities as what they have claimed using some techniques so as to ensure the authenticity. If there is not such an authentication mechanism, the adversary could impersonate a benign node and thus get access to confidential resources, or even propagate some fake messages to disturb the normal network operations.

1.4.4. Non repudiation

Non repudiation ensures that the sender and the receiver of a message cannot disavow that they have ever sent or received such a message.

This is useful especially when we need to discriminate if a node with some abnormal behaviour is compromised or not: if a node recognizes that the message it has received is erroneous, it can then use the incorrect message as an evidence to notify other nodes that the node sending out the improper message should have been compromised.

1.4.5. Authorization

Authorization is a process in which an entity is issued a credential, which specifies the privileges and permissions it has and cannot be falsified, by the certificate authority. Authorization is generally used to assign different access rights to different level of users. For instance, we need to ensure that network management function is only accessible by the network administrator. Therefore there should be an authorization process before the network administrator accesses the network management functions.

1.4.6. Anonymity

Anonymity means that all the information that can be used to identify the owner or the current user of the node should default be kept private and not be distributed by the node itself or the system software. This criterion is closely related to privacy preserving, in which we should try to protect the privacy of the nodes from arbitrary disclosure to any other entities.

II. Attacks in MANET

There are numerous kinds of attacks in the mobile ad hoc network, almost all of which can be classified as the following two types. (ie)

(i) External attacks in which the attacker aims to cause congestion propagate fake routing information or disturb nodes from providing services.

(ii) Internal attacks in which the adversary wants to gain the normal access to the network and participate the network activities, either by some malicious impersonation to get the access to the network as a new node, or by directly compromising a current node and using it as a basis to conduct its malicious behaviours.

2.1. Denial of Service (DoS)

The first type of attack is denial of service, which aims to crab the availability of certain node or even the services of the entire ad hoc networks. In the traditional wired network, the DoS attacks are carried out by flooding some kind of network traffic to the target so as to exhaust the processing power of the target and make the services provided by the target become unavailable. Nevertheless, it becomes not practical to perform the traditional DoS attacks in the mobile ad hoc networks because of the distributed nature of the services. Moreover, the mobile ad hoc networks are more vulnerable than the wired networks because of the interference-prone radio channel and the limited battery power.

2.2. Attacks against Routing

Routing is one of the most important services in the network; therefore it is also one of the main targets to which attackers conduct their malicious behaviours. In the mobile ad hoc networks, attacks against routing are generally classified into two categories: attacks on routing protocols and attacks on packet forwarding/delivery. Attacks on routing protocols aim to block the propagation of the routing information to the victim even if there are some routes from the victim to other destinations. Attacks on packet forwarding try to disturb the packet delivery along a predefined path.

2.3. Intrusion Detection Techniques in MANET

In this paper, a general intrusion detection framework in MANET was proposed, which was distributed and cooperative to meet with the needs of MANET. The architecture of the intrusion detection system is shown below

.

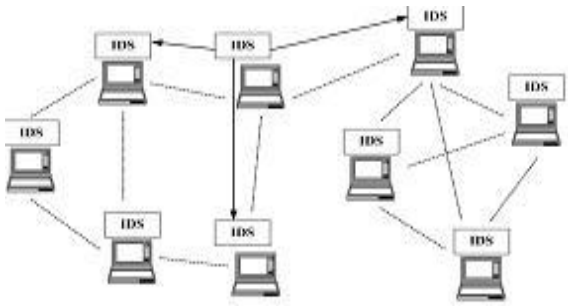

Fig.3. The Architecture of IDS

This is the basic architecture for the MANET. In this architecture, every node in the mobile ad hoc networks participates in the intrusion detection and response activities by detecting signs of intrusion behaviour locally and independently, which are performed by the built-in IDS agent.

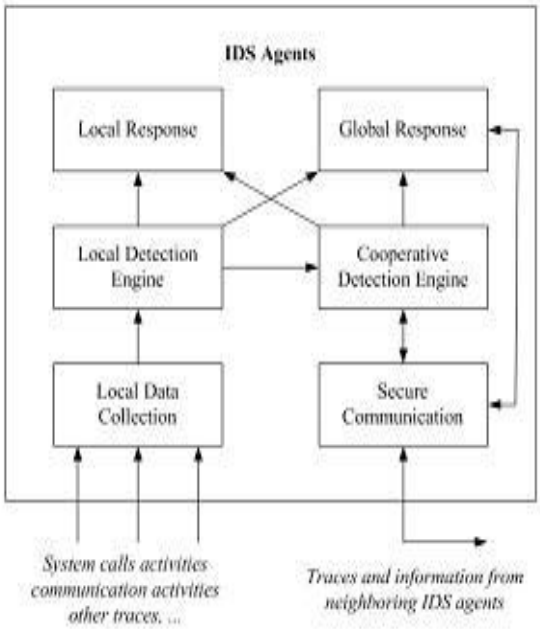

Fig.4. The Agents of IDS

2.4. Secure Routing Techniques in Mobile Ad Hoc Network

As we have discussed in Section there are numerous kinds of attacks against the routing layer in the mobile ad hoc networks, some of which are more sophisticated and harder to detect than others, such as Wormhole attacks and Rush attacks. In this part, we first discuss these two kinds of sophisticated attacks and then we introduce Watchdog and Pathrater which are two main components in a system that aims to mitigate the routing misbehaviours in mobile ad hoc networks . Finally we move to a secure ad hoc routing approach using Localized self-healing communities.

2.5. Defense Mechanism against Rushing Attacks in Mobile Ad Hoc Networks

Rushing attack is a new attack that results in denial-of-service when used against all previous on-demand ad hoc network routing protocols. This attack is also particularly damaging because it can be performed by a relatively weak attacker. The implementation details of rushing attacks are shown in the Figure In the network shown in Figure, the initiator node initiates a Route Discovery for the target node. If the ROUTE REQUESTs for this Discovery forwarded by the attacker are the first to reach each neighbour of the target (shown in gray in the figure), then any route discovered by this Route Discovery will include a hop through the attacker. That is, when a neighbour of the target receives the rushed REQUEST from the attacker, it forwards that REQUEST, and will not forward any further REQUESTs from this Route Discovery. When non-attacking REQUESTs arrive later at these nodes, they will discard those legitimate REQUESTs. As a result, the initiator will be unable to discover any usable routes (i.e., routes that do not include the attacker) containing at least two hops (three nodes).

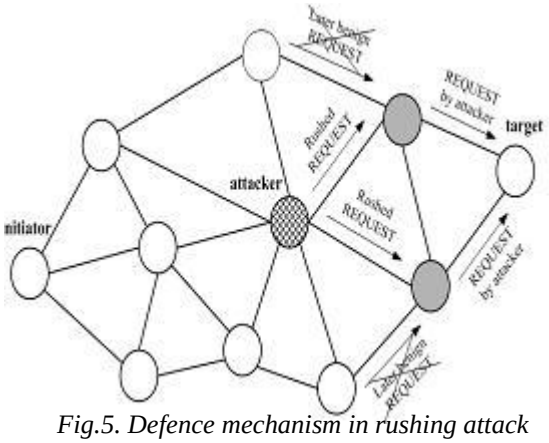

Fig.5. Defence mechanism in rushing attack

III. The Future of Ad hoc Networks

Mobile ad hoc networks are the future of wireless networks because they are practical, versatile, simple, easy to use and inexpensive. We will be living in a world where our network instantly updates and reconfigures itself to keep us connected anywhere we go. These networks provide a new approach for wireless communication and by operating in a license free frequency band prove to be relatively inexpensive. With the current trend of society's demand for information at out fingertips, we will see our future living environments requiring communication networks between the many devices we use in day to day living, allowing them to talk to each other. For example devices like personal digital assistants and mobile phones being able to receive instant messages from a home device. Such as a refrigerator sending a message to a PDA to update its shopping list; notifying that it's run out of milk.

IV. WAND

WAND is a project that is currently in progress to aid research in the area of ad-hoc networks. The project is run by the Distributed Systems Group of Trinity College, in collaboration with Media Lab Europe. WAND is arranged as a large scale test bed for ad-hoc networks protocols and applications, covering a 2km route from Trinity to Media Lab Europe.

This route will be routed with custom-built wireless-enabled embedded PCs. Along this stretch, the embedded PCs will be placed in apartments, shops, on traffic lights and in phone booths providing a minimum level of connectivity. The PCs form a sparse population of wireless network nodes. This sparse coverage is constantly available and the embedded PCs can be configured to create a variety of network models. Other devices with wireless connectivity may also connect to the network via the implementation of mobilenodes.

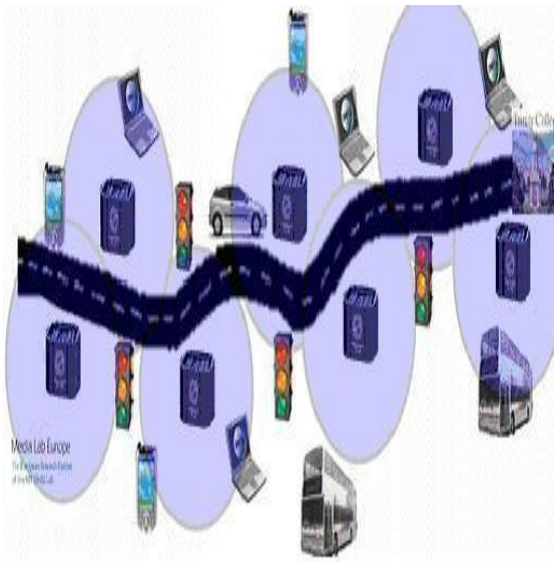

Fig.6. The routing structure of WAND

Many factors lead us to believe that ad-hoc is the wireless network of the future. Due to the network not requiring any base station makes them indispensable in disaster relief situations or military war zones. Also energy issues have moved us from using a single long wireless link to a mesh of short links This proves that an ad-hoc networks will be the future of our wireless networks.

V. Conclusion

After surveying Ad-hoc networks in depth, we believe that they will be the future of wireless networking. It is true that performance suffers as the number of devices grows and large ad-hoc networks become difficult to route and manage. However, much time is being devoted to achieving routing stability, and a few technical issues need to be solved before they become common place. The area of ad hoc networks is a very fast growing area, and due to the vast research in them, we are seeing these problems disappear and they are coming into a world of their own.

References

[1] TiranuchAnantvalee and Jie Wu, "A Survey on Intrusion Detection in Mobile Ad Hoc Networks", Wireless/Mobile Network Security, 2006 Springer.

[2] Ovais Ahmad Khan, "A Survey of Secure Routing Techniques for MANET", http://ovais.khan.tripod.com/papers/Secure_Routing_MANE T.pdf

[3] Ernesto Jiménez Caballero, "Vulnerabilities of Intrusion Detection Systems in Mobile Ad-hoc Networks -The routing problem", http://www.tml.tkk.fi/Publications/C/22/papers/Jimenez_fina l.pdf

[4] Yanchao Zhang, WenjingLouy, Wei Liu and Yuguang Fang, "A Secure Incentive Protocol for Mobile Ad Hoc Networks", Wireless Networks, Springer 2006.

[5] Kejun Liu, Jing Deng, Pramod K. Varshney, and KashyapBalakrishnan, "An Acknowledgment-based Approach for the Detection of Routing Misbehavior in MANETs", IEEE Transactions on Mobile Computing, May 2007.

[6] Gabriela F. Cretu, Janak J. Parekh, Ke Wang and Salvatore J. Stolfo, "Intrusion and Anomaly Detection Model Exchange for Mobile Ad-Hoc Networks", 3rd IEEE Conference on Consumer Communications and Networking, 2006.

[7] AnandPatwardhan, Jim Parker, Anupam Joshi, Michaela Iorga and Tom Karygiannis, "Secure Routing and Intrusion Detection in Ad Hoc Networks", Proceedings of the 3rd International Conference on Pervasive Computing and Communications, IEEE 2005.

[8] S. Madhavi and Tai Hoon Kim, "An Intrusion Detection System in MobileAdhoc Networks", International Journal of Security and Its Applications Vol. 2, No.3, July, 2008.

[9] Angelo Rossi and Samuel Pierre, "Collusion-resistant reputation-based intrusion detection system for MANETs", IJCSNS International Journal of Computer Science and Network Security, VOL.9 No.11, November 2009.

[10] Animesh Kr Trivedi, Rishi Kapoor, RajanArora, SudipSanya and SugataSanya, "RISM - Reputation Based Intrusion Detection System for MobileAdhoc Networks", 3rd International Conference on Computers and Devices for Communication – 2006.

[11] HaiyunLuo, PetrosZerfos, Jiejun Kong, Songwu Lu and Lixia Zhang "Self-securing Ad HocWireless Networks" In Proceedings: ISCC.Year 2002.

[12] S.Dhanalakshmi and Dr.M.Rajaram "A Reliable and Secure Framework for Detection and Isolation of Malicious Nodes in MANET"IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.10, October 2008.