MANETs Security Issues Regarding Attacks

Priyanka Bansal
[1]*Research Scholar (Department of Computer Science & Engineering),*
RIMT-IET, Mandi Gobindgarh (147301), Punjab, India.

Prof. Anuj K. Gupta
[2]*Professor & Head(Department of Computer Science & Engineering),*
RIMT-IET, Mandi Gobindgarh (147301), Punjab, India

Abstract- In this paper, the Manet security issues with regards to attacks will be discussed. Owe to the vulnerable nature of the Manet, there are plentiful security threats that disturbs the development of it. In the past of communication, the presently time span duration has advent the mobile computing which has effectively changed our information society. Applications of adhoc network have a wider range of utilizations such as in military affairs, emergency disaster reliefs and many other several commercial based works such as community networking. Survey of the current security solutions for Manets will be done.

Keywords- MANET, Security, Intrusion Detection, Secure Routing, Attacks

I. INTRODUCTION

The applications and services run by mobile devices such as network connections and corresponding data services are the most demanding. The connections among the wireless devices are achieved via fixed infrastructure-based service provider, or private networks. For example, two cell phones are connected by BSC (Base Station Controller) and MSC (Mobile Switching Center) in cellular networks. When talk about laptops these are connected to Internet via wireless access points. On the other hand infrastructure-based networks provide a great way for mobile devices to get network services; it takes time and sometime potentially high charges to set up the required infrastructure. But except all this there are, some situations where network connections are not available in a given geographic area. So without any physical connection set up providing the needed connectivity and network services in these situations become a real challenge. For all the above reasons, make advancement in technology and standardization, new alternative approach in mobile connectivity. These are dependent on the mobile devices which are also called nodes, connected to each other in the communication range by any automatic relationship. So setting up an ad-hoc mobile network is flexible as well as powerful.

There are different types of wireless networks. The first easiest network topology is, where every hop is capable to influence all the other nodes with the traditional radio relay systems with a big range. There is no usage of routing protocols with these kind of networks because all nodes can see the others nodes. The second kind of protocols also uses the radio relay system but every node has smaller range, therefore the respected hop has to utilize neighboring nodes to be reached at another nodes that is not within its transmission spectrum or range. Then, all other intermediary nodes are the routers.

II. CHARACTERISTICS, COMPLEXITIES and DESIGN CONSTRAINTS

Manets wipe out the constraint of infrastructure set up and enables the agents to generate and join networks on the fly, anywhere, at any time and virtually for any kind of applications. Manets inherit the casual problems of wireless networking in general, and add their own constraints and restrictions specifically to adhoc routing. Some of the notable characteristics, complexities as well as complications and design constraints of MANETs are presented below:

A. Wireless Mediums-

In the adhoc environment, nodes can communicate wirelessly and also share the same media like radio, infrared etc. The wireless mediums has neither absolute, nor readily observable boundaries outside of which stations are unable to receive network frames. Therefore channel as well as medium is not safe from exterior or outside signals and hence it is significantly lesser reliable than the other wired media.

B. Autonomous and Infrastructure Less-
Manets does not depends on the pre-established infrastructure or centralized administration. Every node operates in its distributed peer-to-peer mode that acts as an independent router and produces the independent data. Network management has to be distributed over different nodes, which brings the added difficulties in fault detection and management systems.

C. Dynamic and Changing Network Topologies-
In Manets, because nodes can move arbitrarily, the network topology, which is typically multi-hop, could change frequently and unpredictably as a result there will be route changes, frequent network partitions, and possibly packet losses.

D. Limited Resources Availability-
Due to the limited power supply carried by each mobile node batteries, processing power is limited, which results in limiting the utilities and applications or functions that can be supported by every supported hops. This becomes the bigger issue in MANET, since every hop is acting or behaving as both an end system and a router at the same time respectively, additional energy is required to forward packets.

All the above discussed unique characteristics of ad-hoc networks present many research areas related to security, such as, key management models, secure routing protocols, instruction detection systems and trust based models. This work is based on the research done in the area of secure structured model .In thesis work the term attacks and threats interchangeable will be used.

III. SECURITY ISSUES of EXISTING ROUTING PROTOCOLS

Every kind of routing protocols must encapsulate the crucial set of security mechanisms. There are several mechanisms that help in preventing, detecting, and responding to security attacks. There are majorly five security goals that are needed to be addressed in order to provide a strong and secure adhoc network environment. They are mainly:

A. Confidentiality-
The protection or safety of any kind of information and data from being exposed to malicious entities. In adhoc networks this is very much crucial to attain because intermediates hops (routers) obtain the packets for other recipients or beneficiary, so they can easily eavesdropped the information being routed.

B. Availability-
The services should be available only whenever required. There must be an affirmation of survivability even though a Denial of Service attack which is very crucial attack to detect. At the physical and MAC (media access control) layers, malicious attacker can use the jamming methods to obstructs with communication on physical channel. At network layer, the malicious attacker can spoil the routing protocols. At the higher layers, the malicious attacker could bring down high level of services e.g. key management service (P.G.P- Pretty Good Privacy).

C. Authentication-
The guarantee that an entity of concern or the root of communications is what it asserted to be or from. Without which the malicious attacker would impersonate a node, thus having illegitimate access to resource and sensitive as well as important information or reports and interfering with operation or processing of other nodes.

D. Integrity-
The messages or information being sent can never be altered or changed.

E. Non-Repudiation-
It safeguards that respected sending and receiving parties can never deny the ever sending or receiving the messages and information.

Majorly there are two major categories of malicious attacks while considering any kind of network. The attacks from external or outside sources and attacks from within the network i.e. internal attacks. The second attack i.e. internal attacks are much more crucial to detect and as well as to correct it is also very crucial. So the routing protocols must be able enough to secure themselves against both of these crucial attacks. Adhoc network have wide range of research issues among which security is particularly more challenging and important due to the unique topology and lack of infrastructure support. Till now many security mechanisms has been developed and proposed, but still it is difficult to ensure that whole network is free from any malicious attack.

In future the security issues associated with the existing attacks will be concentrated. In future work first discuss about existing attacker approaches and their attacking methods. Then here will be the new approach, developed with the potential based method of attackers. Also propose an approach in which all attacking potential will be incorporated. This approach will be based on the message-passing & functionality of attacks. The new proposed work represents a technique by which the group of attacks can be dissolved easily.

Wireless nature of MANETs brings always newly security challenges to network design. Manets, due to their unique characteristics, are generally much more accessible to vital information and also physical security based threats than wired networks or infrastructure-based wireless networks.

IV. ANALYSIS of SECURITY ATTACK

Security is an essential as well as crucial service for wired as well as wireless network communications. The huge success of MANETs strongly depends on people's strong confidence in its security. However, the aspects of MANETs pose both challenges as well as opportunities in achieving the min security goals like confidentiality, authentication, integrity, availability, access control, and non-repudiation. So, firstly in this paper an analysis of attacks according to the protocols stacks, and to security aspects and mechanisms is given. Then presented different types of attacks faced by routing protocols. Then presented mainly preventive approaches following the order of the layered protocol stacks. One must forward overview of MANET intrusion detection systems (IDS).

There are a wide variety of attacks that target the weakness of MANET. For example, routing messages are the crucial element of mobile network communications, as each of the packet need to be passed very quickly through intermediate nodes, which the packet must traverse from a source to the destination. Malicious routing attacks can target the routing discovery or maintenance phase by not following the specifications of the routing protocols. There are also attacks that target some particular routing protocols, such as DSR, AODV or AOMDV. Currently routing security is one of the hottest research areas in MANET.

A. Security Attacks-

The attacks in MANET can roughly be classified into two major categories, namely passive attacks and active attacks. A passive attack obtains data exchanged in the network without disrupting the operation of the communications, while an active attack also involves the crucial information interruption, modification, or as well as fabrication, thereby disrupting the normal functionality of a MANET. Examples of passive attacks are eavesdropping, traffic analysis and traffic monitoring. Examples of active attacks include jamming, impersonating, modification, denial of service (DOS), and message replay.

The attacks can also be classified into two categories, namely external attacks and internal attacks, according the domain of the attacks. External or outside attacks are carried out by nodes that do not belong to the domain of the network. Internal attacks are from compromised nodes, which are actually part of the network. Internal attacks are more severe when compared with outside attacks since the insider knows valuable and secret information, and possesses privileged access rights.

B. Types of Attacks Face by Routing Protocols-

Due to the challenged architecture, adhoc networks are more easily attacked by malicious users than in a wired network. The attacks prevailing on adhoc routing protocols can be broadly categorized in passive and active attacks.

A passive attack doesn't spoil the normal operation of protocol, but always tries to discover important information by listening to the traffic. Passive attacks involve obtaining the fundamental routing information or crucial data by sniffing about the network. Such type of attacks are usually very difficult to detected and hence, defending against

such type of attacks is complicated. Even if the case that it is not possible to identify the correct location of a node, intruder may be able to discover or find out the information about the used network topology, using these type of attacks.

An Active Attack, injects the speedily packets and always tries to spoil the normal operation of the protocol in order to have limited availability, also acquire authentication, or drag packets destined to other nodes. The main goal is to drag all the packets to the intruder for analysis or to disable or exhaust the network. But such type of crucial attacks can be detected and the hops can be identified or searched.

V. ATTACKS using DIFFERRENT CLASIFICATIONS

On the basis on network protocol stack, attacks can be classified into following categories (below is a classification of security attacks based on protocol stack; some attacks could be launched at multiple layers):

1. Application layer :Repudiation, Data Corruption Attacks
2. Transport layer :Session Hijacking, SYN Flooding Attacks
3. Network layer: Wormhole, Blackhole, Byzantine, Flooding Attacks
4. Data link layer :Resource Consumption, Location Disclosure Attacks
5. Physical layer: Traffic Analysis, Monitoring, Disruption MAC (802.11)
6. Multi-layer attacks : WEP - Weakness Attacks

VI. CONCLUSION

In this survey paper, inspection of security issues in the Manets, which might be main disturbance to the operation of it is tried. Due to the mobility and open media nature, the Manets are much more prone to all kind of security risks, such as information disclosure, intrusion, or even denial of service. As a result, the security needed in the manets are much more higher than those in the traditional wired networks. First briefly introduction of the basic characteristics of the mobile ad hoc network is discussed. Due to the origin or evolution of the concept, pervasive computing, there is an continuously expansion requirement for the network users to get connecting with the world anytime at any place, which inspires the emergence of the Manet. However, with the convenience that the Manets have brought to us, there are also incrementing security threats for the manet, which need to gain enough attention. Finally introduction of the presently security solutions or methods for the mobile ad hoc networks has discussed. This paper based on the discussion of the security criteria in mobile ad hoc network, which acts as a guidance to the security-related research works in this area. Then talk about the main attack types that threaten the current mobile ad hoc networks. In the end, discussed several security techniques that can help protect the mobile ad hoc networks from external and internal security threats.

During the survey, it has found that some points that can be further explored in the future, such as some aspects of the intrusion detection techniques can get further improved. In the research area these problems will be deeply explored.

REFERENCES

[1] M. G. Zapata and n. Asoka.Securing adhoc routing protocols. In *wise '02: proceedings of the acm workshop on the wireless security*, pages 1–10, new york, usa, 2002. Acm press.93
[2] Wenbo He, Achieving the data privacy aggregation in Wireless sensor networks, University of Illinois at Urbana-Champaign, 2008.
[3] wikipedia.org/wiki/Manet.
[4] Ramachandran and Yasinsac. Limitations about On-Demand Secure Protocols. Information Assurance Workshops in , 2004. Proceedings from the 5th Yearly IEEE SMC, 2004
[5] M. Burrows, Abadi, and Needham. "Logic on Authentication" by ACM Transactions on Computer Systems, 1990.
[6] Issues on Security in Manets- by Survey Wenjia and Anupam Joshi Department of CS and Electrical Engineering University of Maryland, Baltimore County.
[7] P. Papadimitriou and Haas. Secured Routing Protocols in Manets. In the Proceedings of SCS communication Networks and also Distributed Systems Modeling System and Simulation Conference (CNDS), 2002.
[8] Yih-Chun Adrian Perrig, Packet Leashes: Defense against the crucial Wormhole Attacks in Wireless Networks, 2003 IEEE.

[9] Maqsood Razi, Jawaid Quamar, “A Hybrid Cryptography Model for Managing Security in Dynamic Topology of MANET” IEEE 2008.
[10] Antonio Vincenzo Taddeo, Alberto Ferrante, “ Security Service Protocol for MANETs “, IEEE 2009
[11] Payal N. Raj, Prashant B. Swadas. “DPRAODV: ADyanamic Learning System Against Blackhole Attack In Bodv Based Manet.” In: International Journal of Computer Science Issues, Vol.2, pp 54-59, 2009.
[12] C. Kim, E. Talipov, and B. Ahn, "A Reverse AODV Routing Protocol in AdHoc Manet", in Proc.Emerging Directions in Embedded and Ubiquitous Computing, EUC 2006 Seoul, Korea, pp.522-531, 2006.
[13] A. Hamidian, “Study Of Internet Connectivity For Mobile Ad Hoc Networks In NS-2”, Master’s Thesis, Departement Of Communication Systems, Lund Institute Of Technology, Lund University, Sweden, January 2003.
[14] R. F. Sari, A. Syarif, K. Ramli, B. Budiardjo, “Performance Evaluation Of Aodv Routing Protocol On Adhoc Networks Testbed Using PDA”, IEEE Malaysia International Conference On Communications And IEEE International Conference On Networks, Kuala Lumpur, Malaysia,16 -18 November 2005.
[15] Kettaf N, Abouaissa H, Lorenz P, “An efficient heterogeneous key manajement approach for secure multicast communication in ad hoc network”, Springet Telecommunication Syatem, vol 37, pp.29-36, 2008.
[16] Davide Cerri and Alessandro Ghioni, “Securing AODV Protocol : - The A-SAODV Secure Routing Prototype,”Communications Magazine, IEEE In Communications Magazine, IEEE, Vol. 46, No. 2. pp. 120-125, February 2008.
[17] M.G. Zapata, “Secure adhoc on-demand distance vector (SAODV) Routing, Protocol” in proceeding of the ACM workshop on wireless security (WISE), Atlanta, 2002.
[18] Stephan Eichler; Christian Roman; "Challenges of Secure Routing in MANETs: A Simulative Approach using AODV-SEC," Mobile Adhoc and Sensor Systems (MASS), 2006 IEEE International Conference on , vol., no., pp.481- 484, Oct. 2006.
[19] Rasib Hassan Khan , K. M. Imtiaz-ud-Din , Abdullah Ali Faruq , Abu Raihan Mostofa Kamal , Abdul , “ the Secured Adaptive Protocol Suite: Ranked Neighbor Discovery method RND and Security Adaptive AODV (SAAODV),” 5th International Conference on Electrical and Computer Engineering ICECE,Dhaka, Bangladesh.December 2008.
[20] Monis Akhlaq, M. Noman Jafri, Muzammil A. Khan, Baber Aslam, Addressing the Security Concerns of Data Exchange in AODV Protocol. Transactions on Engineering, Computing and Technology, Volume 16 ISSN 1305-5313, pp. 29-33, November 2006.
[21] Shidi Xu, Yi Mu and Willy Susilo, “Authenticated AODV Routing Protocol Using One-Time Signature and Transitive Signature Schemes,” Journal of Networks (JNW) Vol. 1 Issue 1, Academy Publisher, ISSN:1796-2056, pp. 47-53, May 2006.
[22] Shidi Xu, Yi Mu and Willy Susilo, "Online/Offline Signatures and Multisignatures for AODV and DSR Routing Security," Information Security and Privacy (ACISP), 11th Australasian Conference, Lecture Notes in Computer Science, Springer-Verlag, , pp. 99 – 110, 2006.
[23] Xiaoqi Li; Lyu, M.R.; Jiangchuan Liu; , "A trust model based routing protocol for secure ad hoc networks," Aerospace Conference, 2004. Proceedings. IEEE , vol.2, no., pp. 1286- 1295 Vol.2, 6-13 March 2004.
[24] A.Menaka Pushpa M.E, “Trust Based Protected Routing in AODV Routing Protocol,” IMSAA'09 Proceeding of 3rd IEEE international conference on the cyberspace of multimedia services architecture and applications IEEE Press Piscataway, NJ, USA , 2009.
[25] Raza, I.; Hussain, S.A., "A Trust based Security Framework for Pure AODV Network," Information and Emerging Technologies, ICIET 2007. International Conference on , vol., no., pp.1-6, 6-7 July 2007.