A Survey on Security attacks and their prevention over Wireless Ad hoc Network

Navjot Kaur [1], Gurpreet Singh[2]

[1] Dept. of Computer Science and Engg.
YIET.
Yamuna Nagar(Haryana), India.
[2] HOD, Dept. of Computer Science and Engg.
YIET.
Yamuna Nagar(Haryana), India

ABSTRACT

In the last few decades, we have seen the proliferation of wireless communications technologies. Wireless technologies are being widely used today across the globe to support the communications needs of very large numbers of end users. Rapid and automatic establishment of wireless networks and services in the absence of a fixed infrastructure is one of the big challenges of communication. Wireless Ad-hoc networks form a relatively new and very diverse field of research. Wireless Ad-hoc networks are decentralized, self-organizing networks capable of forming a communication network without relying on any fixed infrastructure. Wireless Ad-hoc networks have distinct advantages over traditional communication networks. The main goal of wireless ad hoc networks is to allow a group of communication nodes to set up and maintain a network among themselves, without the support of a base station or a central controller. Nodes in most traditional networks use their resources only for data communications, while the infrastructure runs centralized algorithms in determining optimal network behavior. In contrast, ad hoc and sensor network node resources must support network formation and management activities, in addition to data communication. Security and QoS in ad hoc wireless networks have recently become very important and actively researched topics because of a growing demand to support live streaming audio and video in civilian as well as military applications. The wireless links between nodes are highly susceptible to link attacks, which include passive eavesdropping, active interfering, leaking secret information, data tampering, impersonation, message replay, message distortion, and denial of service. In this paper, we provide a comprehensive overview on different types security flaws and their possible prevention schemes over Wireless Ad hoc Networks.

Keyword : - *QoS, AODV, MANETs.*

I. INTRODUCTION

Wireless networks, whether cellular networks or wireless local area networks, have rapidly become an indispensable part of our life. Evidence of this is the widespread usage of such networks in several areas. In addition, the widespread availability of miniature wireless devices such as PDAs, cellular phones, Pocket PCs, and small fixtures on buildings sensors are one step towards making possible the vision of wireless a reality. Technology under development for wireless ad hoc networks is enabling our march toward this end goal; however the security concerns in wireless networking remains a serious impediment to widespread adoption. Therefore, security of such wireless ad hoc networks is an important area that needs to be addressed if such networks are to be widely used. There are two ways of doing this. One way is for the researchers Security in wireless networks differs markedly from security for their wire line counterparts due to the very nature of the physical medium. To achieve the goal of security and privacy in future mobile communication networks, further research and technology development will be required. The complexity of the problem is greatly compounded when the nodes of the network have to accommodate rapid and unpredictable motion, dynamically altering the connectivity of the network itself [1]. Mobile Ad hoc wireless networks are self-creating, self-organizing, and self-administering. They come into being solely by interactions among their constituent wireless nodes, and it is only such interactions that are used to provide the necessary administration functions supporting such networks.

Figure 1 : Mobile Ad hoc Networks.

A. Security Issues and Challenges

Security is an essential service for wired and wireless network communications. Any network that has to be protected might have weaknesses or vulnerabilities, some or all of which may be targeted by an attacker [2]. Hence, one approach to designing security mechanisms for any network is to look at the threats that the network faces and the attacks possible given the vulnerabilities. The designed security mechanisms should then ensure that the system is secure in the light of these threats, attacks, and vulnerabilities. *Threat* is the means through which the ability or intent of an agent to adversely affect an automated system, facility or operation can be manifested. All methods or things used to exploit a weakness in a network, operation, or facility constitute threat agents. *Vulnerability* is any hardware, firmware, or software flaw that leaves an information system open for potential exploitation. The exploitation can be of various types, such as gaining unauthorized access to information or disrupting critical processing. An *attack* is an attempt to bypass the security controls on a computer. The attack may alter, release, or deny data. The success of an attack depends on the vulnerability of the system and the effectiveness of existing countermeasures. Attacks can be divided into two main categories:

1) Passive Attacks

The attacker just snoops the network without disrupting the network operation. These attacks compromise the confidentiality of the data and tell which nodes are working in promiscuous mode.

i. *Eavesdropping:* It is reading or snooping of messages by an unintended receiver. In MANET, the nodes share a wireless medium so nodes can easily overhear communication of the nodes within its transmission range. This attack can be prevented by using encryption.
ii. *Selfishness:* A selfish node in order to save its battery life and resources does not participate in routing either by dropping the packets or not forwarding them.

2) Active Attacks

Attacks in which attacker disrupts the normal operation of the network by fabricating messages, dropping or modifying packets, replaying packets or tunneling them to other part of the network. Basically the content of passing message is modified. These can be internal attacks and external attacks.

i. ***External attacks:*** In external attack the attacker wants to cause congestion in the network this can be done by the propagation of fake routing information. The attacker disturbs the nodes to avail services [4].
ii. ***Internal attacks:*** In internal attacks the attacker wants to gain the access to network & wants to participate in network activities. Attacker does this by some malicious impersonation to get the access to the network as a new node or by directly through a present node and using it as a basis to conduct the attack [5].

There are four main security problems that need to be dealt with in ad hoc networks:

(1) the *authentication* of devices that wish to talk to each other;

(2) the *secure key establishment* of a session key among authenticated devices;

(3) the *secure routing* in multi-hop networks; and

(4) the *secure storage of (key)data* in the devices.

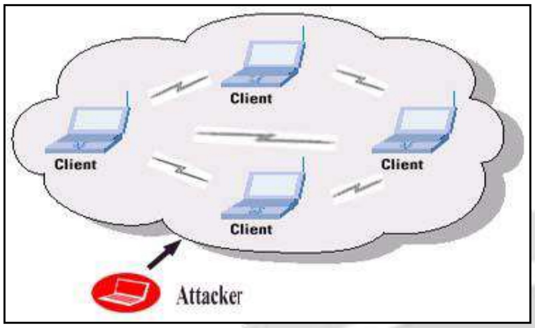

Figure 2: Example of External attack

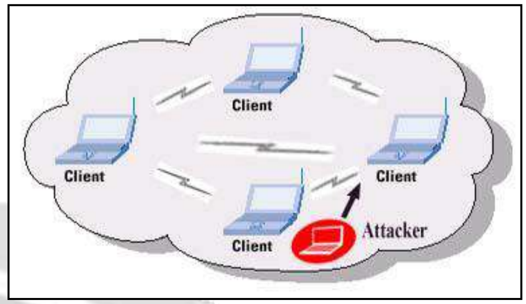

Figure 3: Example of Internal attack

B. Security attributes

Security is the combination of processes, procedures, and systems used to ensure confidentiality, authentication, integrity, availability, access control, and non-repudiation.

- Confidentiality is to keep the information sent unreadable to unauthorized users or nodes. WSN adopts an open medium, so usually all sensor nodes within the direct communication range can obtain the data packets. To keep information confidential, one way is to encrypt the message, and another technique is to use directional antennas.
- Authentication is to be able to identify a node or a user, and to be able to prevent impersonation. In infrastructure-based /wired wireless networks, it is possible to maintain a central authority at a point such as a router, base station, or access point. But there is no central authority in WSN, and it is much more difficult to authenticate an entity.
- Integrity is to be able to keep the message sent from being illegally altered or destroyed in the transmission. When the data packet is sent through the wireless transmission medium, the chunks can be modified or deleted by malicious attacker nodes. The malicious attacker nodes can also resend it, which is called a replay attack.
- Non-repudiation is associated to a fact that if an entity sends some information, the entity cannot deny that the chunks were sent by it. By adopting a signature for these chunks, the entity cannot later deny the chunks. In public key cryptography, a node A signs the packets using its private key. All other nodes can confirms the signed data packets by using A's public key, and A cannot deny that its signature is attached to the message.
- Availability is to keep the network resources or service available to legitimate users. It ensures the sustainability of the network despite malicious incidents.
- Access control is to restrict unauthorized utilization of system resources and network services. Obviously, the access control is bind to authentication attributes. In general, access control is the most commonly thought of service in both network communications and individual computer systems.

C. Security mechanisms

A variety of security mechanisms have been invented to counter malicious attacks. The conventional approaches such as authentication, access control, encryption, and digital signature provide a first line of defense. As a second line of defense, intrusion detection systems and cooperation enforcement mechanisms implemented in MANET can also help to defend against attacks or enforce cooperation, reducing selfish node behavior [6].

- **Preventive mechanism:** The conventional authentication and encryption schemes are based on cryptography, which includes asymmetric and symmetric cryptography. Cryptographic primitives such as hash functions (message digests) can be used to enhance data integrity in transmission as well. Threshold cryptography can be used to hide data by dividing it into a number of shares. Digital signatures can be used to achieve data integrity and authentication services as well. It is also necessary to consider the physical safety of mobile devices, since the hosts are normally small devices, which are physically vulnerable. For example, a device could easily be stolen, lost, or damaged. In the battlefield they are at risk of being hijacked. The protection of the sensitive data on a physical device can be enforced by some security modules, such as tokens or a smart card that is accessible through PIN, passphrases, or biometrics. Although all of these cryptographic primitives combined can prevent most attacks in theory, in reality, due to the design, implementation, or selection of protocols and phys ical device restrictions, there are still a number of malicious attacks bypassing prevention mechanisms.

- **Reactive mechanism:** An intrusion detection system is a second line of defense. There are widely used to detect misuse and anomalies. A misuse detection system attempts to define improper behavior based on the patterns of well-known attacks, but it lacks the ability to detect any attacks that were not considered during the creation of the patterns; Anomaly detection attempts to define normal or expected behavior statistically. It collects data from legitimate user behavior over a period of time, and then statistical tests are applied to determine anomalous behavior with a high level of confidence. In practice, both approaches can be combined to be more effective against attacks. Some intrusion detection systems for MANET have been proposed in recent research papers.

II. RELATED WORK

In [1], Dahill, et al. proposed ARAN, a routing protocol for ad hoc networks that uses authentication and requires the use of a trusted certificate server. In ARAN end-to-end authentication is achieved by the source by having it verify that the intended destination was reached. In this process, the source trusts the destination to choose the return path. The source begins route instantiation by broadcasting a Route Discovery Packet (RDP) that is digitally signed by the source. Following this, every intermediate node verifies the integrity of the packet received by verifying the signature. The first intermediate node appends its own signature encapsulated over the signed packet that it received from the source. All subsequent intermediate nodes remove the signature of their predecessors, verify it and then append their signature to the packet. One primitive solution to vanish the RREP forging is to disable the ability to reply in a message of an intermediate node, so all reply messages should be sent out only by the destination node. This method avoid intermediate node to reply which avoid in certain case the Black Hole and implements the secure protocol. This increase the routing delay in large networks and a malicious node can take advantage by replying message instead of destination node. So for this one or more routes are used by the intermediate nodes which replay the RREQ messages to confirm the routes from intermediate nodes and destination nodes for sending out the data packets. In case if it does not exist, the reply messages is discarded from intermediate node and alarm messages are sent to the network. This method avoids the Black Hole problem thus preventing the network from malicious node. This will result in great delay especially in large networks and in addition the attacker can fabricate a reply message on behalf of the destination node.

In [2], Vinh Hoa LA et al. presents a survey of VANETs attacks and their solutions Risks caused by security attacks are one of the major security issues for the VANETs that are constraining the deployment of the vehicular ad hoc networks. The authors presented an upto- date collection of attacks damaging VANETs, sampled the practical scenarios and also discussed the existing solutions to deal with attacks, and characterized each attack to have a thorough look over it. The authors conclude intruder detection as the better mechanism and intend to construct an intrusion detector for VANETs to alert the attacks in the case performing.

In [3], Bhimsingh Bohara et al. discuss the effect of gray hole attack and their counter measuring solution over mobile adhoc network. The Grayhole attack is an active kind of attack on adhoc networks where the attacking node first forwards packets and then later on drops the packets resulting in Denial of Service (DoS). The author use Intrusion Detection scheme to report violation of policy and the nodes whose packets are dropped again try to establish new paths using Route Requests messages. The Gray hole attack is in a way bit similar to Black hole attack. A black hole attack where drops all the packets, on the other hand the gray hole attacking node drops packet with certain probability. The authors analyzed the effects of gray hole in an AODV network. From simulation results with varying speed and 30 nodes for normal AODV as well as after the inclusion of gray hole in AODV.

In [4], Onkar V.Chandure et al. describe the basic idea related with the implementation of AODV protocol and evaluates the impact of gray hole attack on adhoc network. A Gray hole is a node that selectively drops and forwards data packets after advertises itself as having the shortest path to the destination node in response to a route request message. The authors analyse the impact of gray hole attack on adhoc network for different performance metrices like packet delivery ratio and end to end delay. Simulation of AODV as well as gray hole attack is carried out by using ns-2 simulator.

In [5], Chetan S. Dhamande et al. presented a brief study on different for the minimizing the impact of gray hole attack using AODV routing protocol.. Gray hole attack ultimately decrease the performance of the network & also corrupt the data Proposed solution is mainly focus on the miminize the impact of gray hole attack in MANET & also improve the security as well as the performance of the network. A gray hole may exhibit its malicious behavior in different ways. It may drop packets coming from or destined to certain specific node(s) in the network while forwarding all the packets for other nodes. Another type of gray hole node may behave maliciously for Some time duration by dropping packets but may switch to normal behaviour later.

In [6], Tarun Varshney et al. investigate more existing mechanisms to prevent blackhole attack and propose a slight modification to AODV, called Watchdog –AODV (WAODV) that detects blackhole attack and also attempt to reduce further rise in normalized routing overhead. This mechanism firstly detects a blackhole node and provide a new route to source node. This mechanism greatly increases reliability of detection and isolation of multiple malicious blackhole nodes during route discovery process and discovers a short and secure route towards destination without introducing additional control packets.

In [7], Homgei Deng, Wei Li, and Dharma P. Agarwal proposed a method to surmount the blackhole problem. The scheme assumes that every node that sends a RREP adds also the extra information of the next hop which allows the source to identify the replier's honesty. Therefore, when a source of a RREQ receives a RREP from an intermediate node the source sends an extra request called Further-Request to the next node (information that is known from the RREP that is already received) and examine if the replier has actually a path to the destination. Due to the great overhead that the mechanism introduces the authors suggest its usage only in cases whenever the network finds a suspected node. The authors have not made any simulations of the mechanism's usage thus, factors such as detection time, false positive and false negative are not provided.

In [8], Chang Wu Yu et al. proposed a distributed and cooperative procedure to detect black hole node. In this each node detect local anomalies. It collects information to construct an estimation table which is maintained by each node containing information regarding nodes within power range. This scheme is initiated by the initial detection node which first broadcast and then it notifies all one-hop neighbors of the possible suspicious node. They cooperatively decide that the node is suspicious node. Immediately after the conformation of black hole, the global reaction is activated to establish proper notification system to send warning to whole network. The simulation result show the higher black hole detection rate and achieves better packet delivery. When the network is busier it achieves less overhead.

In [9], Satoshi Kurosawa et al. use an anomaly detection scheme. It uses dynamic training method in which the training data is updated at regular time intervals. Multidimensional feature vector is defined to express state of the network at each node. Each dimension is counted on every time slot.It uses destination sequence number to detect attack. The feature vector include Number of sent out RREQ messages, number of received RREP messages, the average of difference of destination sequence number in each time slot between sequence number of RREP message and the one held in the list. They calculate mean vector by calculating some mathematical calculation. They compare distance between the mean vector and input data sample. If distance is greater than some threshold value then there is an attack. The updated data set to be used for next detection. Repeating this for time interval T anomaly detection is performed.

III. CONCLUSION AND FUTURE WORK

In this paper, We covered general denial of service Various possible threats and attacks on wireless ad hoc networks and their possible prevention. Traditional security mechanisms are generally not suitable for MANETs because it lacks central infrastructure to apply traditional security mechanism such as access control, authentication and trusted third party. Limited bandwidth, battery lifetime, and computation power prohibits the deployment of complex routing protocols or encryption algorithms. Network topologies and memberships are constantly changing. Thus new intrusion detection system and entity recognition mechanisms that are suitable for mobile ad-hoc networks must be designed to avoid or mitigate the behavior to the networks. Trust Management Systems have been recently introduced as a security mechanism in MANETs. In a trust management system, a communicating entity collects evidence regarding competence, honesty or security of other network participants with the purpose of making assessment or decisions regarding their trust relationships.

REFERENCES

[1] K. Sanzgiri, B. Dahill, B.N. Levine, C. Shields, E.M. Belding Royer, “Secure routing protocol for Ad-Hoc networks,” In Proc. of 10th IEEE International Conference on Network Protocols, Dept. of Comput. Sci., California Univ., Santa Barbara, CA, USA. Pp.78- 87, ISSN: 1092-1648, 12-15 Nov. 2002.

[2] Vinh Hoa LA and Ana Cavalli " Security Attacks and Solutions in Vehicular Ad Hoc Networks: A Survey" International Journal on Ad, Hoc Networking Systems (IJANS) Vol. 4, No. 2, April 2014.

[3] Bhimsingh Bohara, Varun Sharma "Analysis and Prevention of effects of gray hole attacks on Routing Protocol in Mobile Ad-hoc Networks" International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 6, June 2013.

[4] Onkar V.Chandure, V.T.Gaikwad "Detection & Prevention of Gray Hole Attack in Mobile Ad-Hoc Network using AODV Routing Protocol" International Journal of Computer Applications, *Volume 41, issue 5 , March 2012*.

[5] Chetan S. Dhamande, H. R. Deshmukh "A Efficient Way To Minimize the Impact of Gray Hole Attack in Adhoc Network" International Journal of Emerging Technology and Advanced Engineering, Volume 2, Issue 2, February 2012.

[6] Tarun Varshney, Tushar Sharmaa, Pankaj Sharma "Implementation of Watchdog Protocol with AODV in Mobile Ad Hoc Network" Fourth International Conference on Communication Systems and Network Technologies, IEEE, Oct. 2014, pp 217-221.

[7]. Hongmei Deng, Dharma P. Argawal, "Routing Security in Wireless Ad Hoc Networks", IEEE Communications Magazine, October 2002.

[8] Chang-Wu Yu, Tung-Kuang Wu, Rei-Heng Cheng, Kun-Ming Yu, Shun Chao Chang: A Distributed and Cooperative Algorithm for the Detection and Elimination of Multiple Black Hole Nodes in Ad Hoc Networks. IEICE Transactions 92-B(2): 483-490 (2009)

[9] Kurosawa, S.; Nakayama, H.; Jamalipour, A.; Nemoto, Y.; Kato, N., "A Dynamic Anomaly Detection Scheme for AODV-Based Mobile Ad Hoc Networks," *Vehicular Technology, IEEE Transactions on* , vol.58, no.5, pp.2471,2481, Jun 2009.